Spring 4-11-2013

PRINCIPAL SERIES REPRESENTATIONS OF GL(2, Qp), AND THEIR CONDUCTORS AND NEWFORMS.

Abdalrazzaq R. Zalloum
ZALLOUM@SIU.EDU

Abdalrazzaq R. Zalloum

PRINCIPAL SERIES REPRESENTATIONS OF $GL(2, \mathbb{Q}_p)$, AND THEIR CONDUCTORS AND NEWFORMS.

by

Abdalrazzaq Zalloum

B.S., Birzeit University, 2011

A Research Paper
Submitted in Algebra as a Requirement for the
Master Degree of Science Degree

Department of Mathematics
Graduate School
Southern Illinois University Carbondale
December, 2012

RESEARCH PAPER APPROVAL

PRINCIPAL SERIES REPRESENTATIONS OF $GL(2, \mathbb{Q}_p)$, AND THEIR CONDUCTORS AND NEWFORMS.

By

Abdalrazzaq Zalloum

A Research Paper Submitted in Partial

Fulfillment of the Requirements

for the Degree of

Master of Science

in the field of Mathematics

Approved by:

Joseph Hundley

Robert Fitzgerald

Dubravka Ban

Graduate School
Southern Illinois University Carbondale
March 24, 2013

TABLE OF CONTENTS

INTRODUCTION

In this paper we find basis for a specific vector space that we will introduce later on. In chapter 1, we make a general review of some abstract algebra and topology. In chapter 2, we define the absolute value on a field in general and we introduce a new type of absolute values called the $p-$ adic absolute value. In chapter 3 we define the vector space $V(\chi_1, \chi_2)$ and we get a good understanding of its elements. Finally, in chapter four, we define the subspace $V(\rho, k)$ of the vector space $V(\chi_1, \chi_2)$. The elements of the subspace $V(\rho, k)$ are called newforms and the least k such that the subspace $V(\rho, k)$ is not trivial is called the conductor of ρ. In chapter 4, we find the conductor and the newforms of the subspace $V(\rho, k)$.

CHAPTER 1

REVIEW OF SOME NOTIONS OF TOPOLOGY AND ABSTRACT ALGEBRA

1.1 SOME TOPOLOGY

In this section we shall introduce some topology background to understand what we will do on the next chapter.

Definition. A topology on a set X is a collection τ of subsets of X such that

(1) $X, \phi \,\epsilon\, \tau$,

(2) The union of elements of any sub-collection of τ is back in τ,

(3) The intersection of the elements of any finite sub-collection of τ is back in τ.

If τ is a topology on a set X then we say that the pair (X, τ) is a topological space.

Definition. Let X be a set with topology τ and let U be subset of X. Then U is said to be open (with respect to the topology τ as of course we might have more than one topology defined on the same set) if U is an element of τ.

Definition. Let X be a set with topology τ. Then a neighborhood of an element $x \in X$ is an open set U such that $x \in U$.

Remark. In general a set X might have more that one topology defined on it, and hence, whenever we mention that a set is open we should clarify with respect to which topology it is open. However, for most of the cases, we will be having only one topology τ on X, and hence, open will mean τ-open (open with respect to the topology τ).

Definition. Given a set X. The discrete topology on X is defined to be the collection of all subsets of the set X, i.e., the discrete topology on X is defined by letting every subset of X be open and X is a discrete topological space if it is equipped with its discrete topology. On the other hand, X is a non-discrete topological space if it is equipped with a topology that is not discrete.

Definition. Let X be a set, a basis for a topology on X is a collection β of subsets of X (called basis elements) such that:

(1) $\forall x \,\epsilon\, X \,\exists\, B \,\epsilon\, \beta$ such that $x \,\epsilon\, B$,

(2) If $x \,\epsilon\, B_1 \bigcap B_2$ then $\exists\, B_3$ such that $x \,\epsilon B_3 \subseteq B_1 \bigcap B_2$.

Remark. Given a basis β, we can define a topology τ on X as follows:

The subset U is open in X if $\forall\, x \,\epsilon\, U \,\exists\, B \,\epsilon\, \beta$ such that $x \,\epsilon\, B \subseteq U$ (note that the basis elements themselves are open, i.e., they are elements of τ).

This topology is called the topology generated by β.

Lemma 1.1.1. *Let X be any set, and let β be a basis for this topology. Then any open set U in the topology generated by β can be written as union of some elements from β.*

Proof. Let U be an open set in this topology, then, $\forall\, x \,\epsilon\, U \,\exists\, B_x$ such that $x \,\epsilon\, B_x \subseteq U$which implies $x \,\epsilon \bigcup_{x \,\epsilon\, U} B_x$, therefore $U \subseteq \bigcup_{x \,\epsilon\, U} B_x$. Now, since we have $B_x \subseteq U$ for each x, then

$$U = \bigcup_{x \,\epsilon\, U} B_x.$$

□

Definition. Let X and Y be two topological spaces, then a function f: $X \to Y$ is said to be continuous if $\forall$ open set $V \subseteq Y$ we have $f^{-1}(V)$ is open in X.

Lemma 1.1.2. *Let X and Y be topological spaces, then the function $f : X \to Y$ is continuous if and only if $\forall\, x \,\epsilon\, X$ and each neighborhood V of $f(x) \,\exists$ a neighborhood U of$x$ such that $f(U) \subseteq V$.*

Proof. Let $f : X \to Y$ be continuous and let x be in X and let V be an open set containing $f(x)$ in Y, now since f is continuous $f^{-1}(V)$ is open in X and we know from set theory that $f(f^{-1}(V)) \subseteq V$ so let's take our U to be the open set $f^{-1}(V)$ and then we are done. Now suppose that $\forall\, x \,\epsilon\, X$ and each neighborhood V of $f(x) \,\exists$ a neighborhood U of x such

that $f(U) \subseteq V$. We claim that if V is open then $f^{-1}(V)$ is open as well. Let V be an open set in Y then $\forall\, x \,\epsilon\, f^{-1}(V)\, \exists\, U_x$ open and containing x such that $f(U_x) \subseteq V$. This implies that $f^{-1}(f(U_x)) \subseteq f^{-1}(V)$. But we know from set theory that $U_x \subseteq f^{-1}(f(U_x))$ or $U_x \subseteq f^{-1}(V)$ and this is true for each x, and it is obvious that $f^{-1}(V) \subseteq \bigcup_{f(x)\,\epsilon\, V} U_x$. This implies that $f^{-1}(V) = \bigcup_{f(x)\,\epsilon\, V} U_x$ where each of those U_x is open and so their union and so $f^{-1}(V)$. □

Definition. A set G is a topological group if G is a group that is equipped with a topology that makes the following functions continuous:

(1) $f : G \times G \to G$ by $f(a, b) = ab$,

(2) $g : G \to G$ by $g(a) = a^{-1}$.

It is not hard to see the following two remarks from the previous definition:

(1) Given $a, b \,\epsilon\, G$ and given V an open set that contains ab, then $\exists\, U_1\,, U_2$ open such that $f\,(U_1, U_2) = U_1U_2 = \{u_1u_2 \mid u_1 \,\epsilon\, U_1\,,\, u_2 \,\epsilon\, U_2\} \subseteq V$,

(2) If $a \,\epsilon\, G$ and if V is any open set containing a^{-1}, then $\exists\, U$ open containing a such that $g\,(U) = U^{-1} = \{u^{-1} \mid u \,\epsilon\, U\} \subseteq V$.

Definition. A metric d on a set is a function $d : X \times X \to \mathbb{R}$ such that:

(1) $d(x, y) \geq 0$ with equality if and only if $x = y$,

(2) $d(x, y) = d(y, x)$,

(3) $d(x, z) \leq d(x, y) + d(y, z)$,

and that is $\forall\; x\,, y\,, z \in X$.

Definition. The $\epsilon - ball$ centered at x with respect to the metric d is defined by:

$$B_d\,(x, \epsilon) = \{y \in X \;\; such \;\; that \;\; d(x, y) < \epsilon\}.$$

Now, we can define a topology τ on X by taking our basis to be the set of all $\epsilon - ball$'s, i.e.,

$$\beta = \{B_d\,(x, \epsilon) \;\; such \; that \; \epsilon > 0 \;, x \in X\}.$$

Therefore, $U \subseteq X$ is a τ-open set if and only if U can be written as a union of elements in β. And since we are almost always dealing with the same metric on the set, there is no need to mention d all the time, we can just refer to the $\epsilon - ball$ centered at x by $B(x, \epsilon)$ or

$$B_\epsilon(x).$$

Definition. Suppose that τ and τ' are two topologies on a given set X. If $\tau \subseteq \tau'$, we say that τ' is finer than τ; if τ' contains τ properly, we say that τ' is strictly finer than τ. We also say that τ is coarser that τ', or strictly coarser that τ', in these two respective situations. We say that τ is comparable with τ' if $\tau \subseteq \tau'$ or $\tau' \subseteq \tau$.

Definition. Let X be a topological space and let $K \subseteq X$. Then K is said to be compact if every open cover containing K has a finite subcover that contains K. Explicitly, this means that for every arbitrary collection:

$$\{U_\alpha\}_{\alpha \in A}$$

of open subsets of X such that

$$K \subseteq \bigcup_{\alpha \in A} U_\alpha,$$

there is a finite subset J of A such that

$$K \subseteq \bigcup_{i \in J} U_i.$$

1.2 SOME ABSTRACT ALGEBRA

In this section we shall introduce some abstract algebra background to understand what we will do on the next chapter. This material is from [2] and [4].

Definition. Let G be a group. A subgroup N of G is said to be normal if $\forall g \in G$, we have $g^{-1}Ng \in N$.

Definition. An action of G on a set X is a mapping $\alpha : G \times X \to X$ that is compatible with the group laws, in the sense that:
(1) $\alpha(gh, x) = \alpha(g, \alpha(h, x))$,
(2) $\alpha(e, x) = x$, for all $g, h \in G$ and $x \in X$, where e is the identity element of G.

Definition. Let G be a group acting on a set X. Let $x \in X$ be given, we define the stabilizer of x in G by:

$$G_x = \{g \in G \mid gx = x\}.$$

Definition. Let G be a group acting on a set X, and suppose $x \in X$. Then, x is said to be invariant by $H \subseteq G$ if $H \subseteq G_x$, i.e., if

$$\alpha(h, x) = x \qquad \forall\ h \in H \subseteq G.$$

Definition. Let G be a group acting on a set X, then the set X^G is defined to be:

$$X^G = \{x \in X \ \mid \ gx = x,\ \forall g \in G\}.$$

Definition. Let H_1, H_2 be subgroups of a group G. For $g \in G$. Define the double coset by:

$$H_1 g H_2 = \{h_1 g h_2 \mid h_1 \in H_1\, h_2 \in H_2\}.$$

Lemma 1.2.1. *Let H_1, H_2 be subgroups of a given group G. And let g, $g^{'} \in G$, then $H_1 g H_2 = H_1 g^{'} H_2$ if and only if $g \in H_1 g^{'} H_2$.*

Proof. As H_1, H_2 are subgroups, we have $e \in H_1$ and $e \in H_2$. Then, $g = ege \in H_1 g H_2 = H_1 g^{'} H_2$. Conversely, suppose that $g \in H_1 g^{'} H_2$. This implies $g = h_1 g^{'} h_2$ where $h_1 \in H_1, h_2 \in H_2$. Now, let $x \in H_1 g H_2$, then $x = h_1^{'} g h_2^{'}$ where $h_1^{'} \in H_1, h_2^{'} \in H_2$. Hence, $x = h_1^{'} g h_2^{'} = h_1^{'} h_1 g^{'} h_2 h_2^{'}$ where $h_1^{'} h_1 \in H_1$ and $h_2 h_2^{'} \in H_2$ (since H_1 and H_2 are subgroups). Therefore, $x \in H_1 g^{'} H_2$. As x is arbitrary, we have

$$H_1 g H_2 \subseteq H_1 g^{'} H_2.$$

Now, the other inclusion is satisfied by symmetry. Hence

$$H_1 g^{'} H_2 \subseteq H_1 g H_2,$$

so

$$H_1 g H_2 = H_1 g^{'} H_2.$$

□

Definition. Let H_1, H_2 subgroups of a given group G, then the set of all double cosets is defined to be the set

$$H_1 \setminus G / H_2 = \{H_1 g H_2 \ \mid \ g \in G\}.$$

Lemma 1.2.2. *Let H_1, H_2 subgroups of a given group G, and let $g, g^{'} \in G$, then*

$$H_1 g H_2 \bigcap H_1 g^{'} H_2 = \emptyset \ \text{ or } \ H_1 g H_2 = H_1 g^{'} H_2.$$

Proof. Assume that $H_1 g H_2 \bigcap H_1 g^{'} H_2 \neq \emptyset$, then $\exists\, x = h_1 g h_2 = h_1^{'} g^{'} h_2^{'}$. Hence, $h_1^{-1} h_1^{'} g^{'} h_2^{'} h_2^{-1} = g$,i.e., $g \in H_1 g^{'} H_2$. Therefore, by lemma 1.2.1, we have $H_1 g H_2 = H_1 g^{'} H_2$. □

One of the obvious results of this lemma is that the group G is equal to a disjoint union of elements from $H_1 \setminus G / H_2$.

CHAPTER 2

ABSOLUTE VALUE ON A FIELD AND P-ADIC NUMBERS

2.1 ABSOLUTE VALUES ON A FIELD

Definition. Let $\mathbb{F}$ be any field. Then an absolute value on $\mathbb{F}$ is a non-negative function $||$ such that:

(1) $|x| = 0$ if and only if $x = 0$,

(2) $|xy| = |x||y|\,, \forall\, x,\, y \,\epsilon\, \mathbb{F}$,

(3) $|x + y| \leq |x| + |y|\,, \forall\, x,\, y \,\epsilon\, \mathbb{F}$.

Remark. If an absolute value satisfies the additional condition $|x+y| \leq \max(|x|,\, |y|)$, then it is called a non-archimedean absolute value.

Definition. The trivial absolute value on any field $\mathbb{F}$ is defined by the following:

$$|x|_{trivial} = \begin{cases} 1, & x \neq 0, \\ 0, & x = 0. \end{cases}$$

Lemma 2.1.1. *Let $\mathbb{F}$ be a field. Then $|1| = 1$.*

Proof. $|1| = |1.1| = |1|.|1|$, and since $1 \neq 0$, $|1| \neq 0$. By dividing both of the sides by $|1|$ we have $|1| = 1$. □

Lemma 2.1.2. *Let $\mathbb{F}$ be a finite field, then if $a \neq 0$, $a \,\epsilon\, \mathbb{F}$, then $a^n = 1$ for some $n \,\epsilon\, \mathbb{N}$.*

Proof. Let $\mathbb{F}$ be finite field, and let $a \neq 0$, $a \,\epsilon\, \mathbb{F}$ then consider the sequence a, a^2, a^3, ..., a^i, ... we must have $a^i = a^j$ for some $i \neq j$ (without loss of generality say $i > j$) since otherwise this sequence will be infinite. Now, we have $a^i = a^j$ for some $i > j$ and since any nonzero element has an inverse, then we have $a^{i-j} = 1$. Now, take $n = i - j$. Then we have $a^n = 1$ and we are done. □

Lemma 2.1.3. *The only possible absolute value on a finite field* $\mathbb{F}$ *is the trivial one.*

Proof. Let $\mathbb{F}$ be a finite field. Let $||$ be an absolute value on $\mathbb{F}$. We should prove that$||$ is the trivial absolute value. First note that $|0| = 0$ since $||$ is an absolute value. Let $a \neq 0$ be in $\mathbb{F}$. Then by the previous lemma, we have $a^n = 1$ for some $n \,\epsilon\, \mathbb{N}$. Now, by lemma 2.1.1, we have $|1| = 1$. Therefore, we have $1 = |1| = |a^n| = |a.a....a|\, n - times = |a|^n$ and hence we have $|a|^n = 1$. Since $||$ is non-negative, then the only possible solution for $|a|^n = 1$ is $|a| = 1$. Because a is arbitrary, we have

$$|a|_{trivial} = \begin{cases} 1, & a \neq 0, \\ 0, & a = 0, \end{cases}$$

which is the trivial absolute value. □

Definition. Let $\mathbb{Q}$ be the field of rational numbers, let $x \,\epsilon\, \mathbb{Q}$ and define the infinity absolute value by the following:

$$|x|_\infty = \begin{cases} x, & x \geq 0, \\ -x, & x < 0. \end{cases}$$

Fix a prime p. We will introduce a new type of absolute value on $\mathbb{Q}$ which is called the p absolute value and we denote it by $||_p$. Given a nonzero $a \in \mathbb{Q}$, we can write a as $a = p^k \frac{m}{n}$ where $m, n, k \in \mathbb{Z}$, $n \neq 0$ and p doesn't divide mn. Then, $|a|_p = p^{-k}$ and $|0|_p = 0$.

Lemma 2.1.4. *Fix a prime* p*. Then* $||_p$ *on* $\mathbb{Q}$ *is an absolute value.*

Proof. (1) We have $|0| = 0$ by definition. Conversely, 0 is the only element with $|0| = 0$ since if any other nonzero $x \in \mathbb{Q}$ satisfies $|x|_p = 0$ then $p^i = 0$ for some $i \in \mathbb{Z}$ which is not possible.

(2) Let x, y be elements of $\mathbb{Q}$, then $x = p^i \frac{m_1}{n_1}$ and $y = p^j \frac{m_2}{n_2}$ where $m_1, m_2, n_1, n_2, i, j \in \mathbb{Q}$ and

p doesn't divide $m_1m_2n_1n_2$. Then, $xy = p^{i+j}\frac{m_1m_2}{n_1n_2}$ and hence $|xy|_p = p^{-(i+j)} = p^{-i}.p^{-j} = |x|_p|y|_p$.

(3) Let x, y be elements of $\mathbb{Q}$. Then, $x = p^i\frac{m_1}{n_1}$ and $y = p^j\frac{m_2}{n_2}$ where $m_1, m_2, n_1, n_2, i, j \in \mathbb{Q}$ and p doesn't divide $m_1m_2n_1n_2$. Now, if $i = j$ then we have $|x+y|_p = |p^i|_p||\frac{1}{n_1n_2}|_p.|m_1n_2 + n_1m_2|_p$. Now, $m_1n_2+n_1m_2$ is an element of $\mathbb{Z}$ and so $m_1n_2+n_1m_2 = p^km$ where $k \geq 0$ and $gcd(m, p) = 1$, therefore, $|m_1n_2 + n_1m_2|_p = p^{-k}$ and hence $|x + y|_p = |p^i|_p||\frac{1}{n_1n_2}|_p.|m_1n_2 + n_1m_2|_p = p^{-i}p^{-k} \leq p^{-i} = |x|_p$. Now, if $i \neq j$, then without loss of generality say $i < j$ (which is equivalent to saying $|x|_p > |y|_p$) and then $|x+y|_p = |p^i|_p||\frac{1}{n_1n_2}|_p.|m_1n_2+n_1m_2p^{j-i}|_p$ where $|m_1n_2 + n_1m_2p^{j-i}|_p = 1$, since otherwise, we will have p divides $m_1n_2 + n_1m_2p^{j-i}$ and so p divides m_1n_2 which is not possible. Therefore, $|x + y|_p = |p^i|_p||\frac{1}{n_1n_2}|_p.|m_1n_2 + n_1m_2p^{j-i}|_p = p^{-i}.1.1 = p^{-i} = |x|_p$. □

Remark. Part 3 proves that $||_p$ is a non-archimedean absolute value as well. In particular, it proves that if x, $y \in \mathbb{Q}$ such that $|x|_p > |y|_p$, then $|x + y|_p = |x|_p$. In other words, the *stronger* wins.

Definition. The numbers 2,3,5,7,11,... are called finite primes and ∞ is called the infinite prime.

Theorem 2.1.5. *Let $x \in \mathbb{Q}$ be a nonzero element, then*

$$\prod_v |x|_v = 1,$$

where the product is taken over all the finite and the infinite primes.

Proof. Let x be a nonzero element in $\mathbb{Q}$. If x is positive, then $x = \frac{m}{n}$ with $gcd(m, n) = 1$. Then, from number theory we can write $m = p_1^{\alpha_1}p_2^{\alpha_2}...p_l^{\alpha_l}$ and $n = q_1^{\beta_1}q_2^{\beta_2}...q_k^{\beta_k}$ where p_i's and q_i's are finite primes and the α's and the β's are positive integers. Then, we have

$$x = \frac{p_1^{\alpha_1}p_2^{\alpha_2}...p_l^{\alpha_l}}{{q_1}^{\beta_1}q_2^{\beta_2}...q_k^{\beta_k}},$$

or

$$x = p_1^{\alpha_1} p_2^{\alpha_2} ... p_l^{\alpha_l} {q_1}^{-\beta_1} q_2^{-\beta_2} ... q_k^{-\beta_k},$$

and then $|x|_{p_i} = p_i^{-\alpha_i}$, $|x|_{q_i} = q_i^{\beta_i}$ and $|x|_p = 1$ provided that p doesn't divide mn. Since $x > 0$, we have $|x|_\infty = x$. Therefore,

$$\prod_{All\, finite\, primes\, p} |x|_p = p_1^{-\alpha_1} p_2^{-\alpha_2} ... p_l^{-\alpha_l} {q_1}^{\beta_1} q_2^{\beta_2} ... q_k^{\beta_k} = \frac{1}{x},$$

and $|x|_\infty = x$ as $x > 0$. This implies that

$$\prod_{v\, such\, that\, v\, is\, prime} |x|_v = \frac{1}{x}.\, x = 1.$$

If $x < 0$, then $-x > 0$. Now, for each prime p, the highest power of p that divided x is the same as the highest power of p that divides $-x$ (if $x = \frac{-m_1}{n_1} p^j$ then $-x = \frac{m_1}{n_1} p^j$). Hence, for any prime p, we have $|x|_p = |-x|_p$. Now, as $-x \in \mathbb{N}$, we can write it as $-x = p_1^{\alpha_1} p_2^{\alpha_2} ... p_l^{\alpha_l} {q_1}^{-\beta_1} q_2^{-\beta_2} ... q_k^{-\beta_k}$, where p_i's and q_i's are finite primes and the α's and the β's are positive integers. Hence,

$$\prod_{All\, finite\, primes\, p} |x|_p = \prod_{All\, finite\, primes\, p} |-x|_p = p_1^{-\alpha_1} p_2^{-\alpha_2} ... p_l^{-\alpha_l} {q_1}^{\beta_1} q_2^{\beta_2} ... q_k^{\beta_k} = \frac{1}{-x}.$$

Now, as $x < 0$, then we have $|x|_\infty = -x$. This implies that

$$\prod_{v\, such\, that\, v\, is\, prime} |x|_v = \frac{1}{-x}.\, -x = 1.$$

□

Example 2.1.1. Finding a sequence that converges to zero in the 7-adic.

Take

$$x_n = 7^n,$$

then

$$|x_n|_7 = 7^{-n} \to 0.$$

Example 2.1.2. Finding a sequence that converges to 32 in the 7-adic.

We want $|x_n - 32|_7 \to 0$. Hence, a smart choice of x_n will do it. Choose $x_n = 32(7^n + 1)$ and then

$$|x_n - 32|_7 = |32.7^n + 32 - 32|_7 = |32.7^n|_7 = |32|_7|7^n|_7 = 1.7^{-n} \to 0.$$

The previous two examples are taken from [2].

2.2 COMPLETION AND P-ADIC NUMBERS

Once one has an absolute value on a field $\mathbb{F}$, one has a metric $d(x, y) = |x - y|$.. Hence, one may start thinking of convergence of sequences. Considering this, the notion of a Cauchy sequence arise, these are the sequences were their terms are getting "closer and closer" to each others with respect to a given absolute value. The process of extending the field so that every Cauchy sequence converge is called completion of the field. The material in the section is taken from [6].

Definition. Let $\mathbb{F}$ be a field, and let x_n with $n \in \mathbb{N}$ be a sequence in $\mathbb{F}$, then this sequence is called Cauchy sequence provided that

$$\forall \epsilon > 0 \ \exists\, k \in N \text{ such that } \forall\, m,\, n > k \ \text{ we have } \ |x_n - x_m| < \epsilon.$$

In other words, that means as n gets larger, the sequence terms get closer and closer to each other with respect to the absolute value defined on that field.

Definition. The field $\mathbb{F}$ is called complete if every cauchy sequence converges to an element in the field.

Lemma 2.2.1. *The field of rational numbers with the p absolute value is not complete.*

Proof. We know from number theory that for each $i \in \mathbb{N}$, there is a natural number n_i such that $6 \equiv n_i^2 \mod 5^i$. Now, define the sequence $x_i := n_i$ and assume for the sake

of contradiction that $x_i \to x \in \mathbb{Q}$ in the 5-absolute value, and then we have $|6 - x^2|_5 = \lim_{i\to\infty} |6 - n_i^2|_5$. Since 5^i divides $6 - n_i^2$ for each $i \in \mathbb{N}$, then $|6 - n_i^2| \leq 5^{-i} \to 0$ for each i in $\mathbb{N}$. Hence, $|6 - x^2|_5 = 0$ or $6 = x^2$ a contradiction as $x \in \mathbb{Q}$. □

Definition. Let $\mathbb{F}$ be field with an absolute value $|\ |$ defined on it. The following process is defined to be the *completion* of the field $\mathbb{F}$ with respect to the given absolute value $|\ |$. Let X be the set of all Cauchy sequences in the field $\mathbb{F}$. Define a relation R on X by the following:

$$x_n \, R \, y_n \ \text{ if and only if } \lim_{n\to\infty} |x_n - y_n| = 0.$$

Now, let M denote the set of all these equivalence classes arising from the relation R where the equivalence of a sequence $x_n \in \mathbb{F}$ is denoted by $[x_n]$. Then, M is the completion of the field $\mathbb{F}$ and the original elements $a \in F$, can be realized in M as the equivalence class represented by the constant sequence $a, a, a, \ldots$. In the new field M, addition, subtraction and multiplication are defined as following

$$[x_n] + [y_n] = [x_n + y_n],$$

$$[x_n] - [y_n] = [x_n - y_n],$$

$$[x_n].[y_n] = [x_n.y_n],$$

for all Cauchy sequences $x_n, y_n \in \mathbb{F}$. Now, let z_n be a nonzero Cauchy sequence in $\mathbb{F}$, then division is defined as following

$$1/[z_n] = [1/z_n],$$

here we should be a little aware as even if the sequence z_n is non-zero, some of its terms might still be zeros, however, any non-zero Cauchy sequence is related (under the previous relation) to some Cauchy sequence where none of its terms is zero, hence z_n can be replaced with a representative with no zero terms.

Remark. The completion of the field $\mathbb{Q}$ with respect to $|\ |_\infty$ is the field of real number $\mathbb{R}$.

Definition. The field $\mathbb{Q}_p$ is defined to be the field resulted from completing the field $\mathbb{Q}$ with respect to the p-absolute value $|\ |_p$.

Definition. The set $\mathbb{Z}_p$ is defined to be the set of all elements of the form:

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \ | \ |x|_p \leq 1\}.$$

Remark. Note that the elements in $\mathbb{Q}_p$ are represented by sequences, and then, when we say that an element x_n of $\mathbb{Q}_p$ satisfies $|x_n|_p \leq 1$ we mean by that $\exists\ k \in \mathbb{N}$ such that $|x_n|_p \leq 1$ for all $n \geq k$.

Lemma 2.2.2. *The set $\mathbb{Z}_p$ is actually an integral domain, and each element contains a unique Cauchy sequence of the form:*

$$\sum_{i=0}^{\infty} a_i p^i = (\sum_{i=0}^{n} a_i p^i)_{n=1}^{\infty},$$

where $a_i \in \{0, 1, 2, ..., p-1\}$. Each element of the field $\mathbb{Q}_p$ contains a unique Cauchy sequence of the form:

$$\sum_{i=-k}^{\infty} a_i p^i = (\sum_{i=-k}^{n} a_i p^i)_{n=1}^{\infty},$$

with $k \in \mathbb{N}, a_i \in \{0, 1, 2, ..., p-1\}$.

Remark. From the previous lemma we can see that if $x \in \mathbb{Q}_p$ such that $x = \sum_{i=-k}^{\infty} a_i p^i$ with $k \in \mathbb{N}, a_i \in \{0, 1, 2, ..., p-1\}$, then the p-absolute value of this element is $|x|_p = p^{-d}$ where a_d is the first nonzero term in the sum (d might be positive or negative). Hence, if $x \in \mathbb{Z}_p$ such that $x = \sum_{i=0}^{\infty} a_i p^i$, with $a_i \in \{0, 1, 2, ..., p-1\}$, then $|x|_p = 1$ if and only if $a_0 \neq 0$.

Lemma 2.2.3. *Define the set $p\mathbb{Z}_p$ by:*

$$p\mathbb{Z}_p = \{px \ | \ x \in \mathbb{Z}_p\}.$$

Then we have

$$p\mathbb{Z}_p = \{x \in \mathbb{Z}_p \, such \, that \, |x|_p < 1\}.$$

Proof. Let $x \in p\mathbb{Z}_p$. Then $x = py$, where $y \in \mathbb{Z}_p$ which implies $|x|_p = |py|_p = |p|_p|y|_p \leq \frac{1}{p}.1 < 1$. Conversely, let $x \in \mathbb{Z}_p$ such that $|x|_p < 1$, then the possibilities for the absolute value are $\frac{1}{p}$, $\frac{1}{p^2}$, ...$\frac{1}{p^i}$..., hence, $x = \sum_{i=0}^{\infty} a_i p^i$ with $a_0 = 0$ (since otherwise $|x|_p = 1$). Now, let j be the first index where $a_j \neq 0$, then $x = a_j p^j + a_j p^{j+1} + ...$, where $j \geq 1$. Therefore, $x = p(a_j p^{j-1} + a_{j+1} p^j + ...)$, where $|a_j p^{j-1} + a_{j+1} p^j + ...|_p = p^{1-j} \leq 1$. Thus, $y := a_j p^{j-1} + a_{j+1} p^j + ... \in \mathbb{Z}_p$ which implies $x = py$, where $y \in \mathbb{Z}_p$. We conclude that $x \in p\mathbb{Z}_p$. □

Lemma 2.2.4. *The units in $\mathbb{Z}_p$ are*

$$\mathbb{Z}_p^{\times} = \{x \in \mathbb{Z}_p \mid |x|_p = 1\}.$$

Proof. Let $x \in \mathbb{Z}_p$ such that $x^{-1} \in \mathbb{Z}_p$, then $1 = |1|_p = |xx^{-1}|_p = |x|_p|x^{-1}|_p$. Therefore, $|x^{-1}|_p = \frac{1}{|x|_p}$. Now, since both x and x^{-1} are in $\mathbb{Z}_p$, we have $|x|_p \leq 1$ and $|x^{-1}|_p \leq 1$ or $|x|_p \leq 1$ and $\frac{1}{|x|_p} \leq 1$ and hence $|x|_p \leq 1$ and $|x|_p \geq 1$ which can't be true unless $|x|_p = 1$. Conversely, let $x \in \mathbb{Z}_p$ be such that $|x|_p = 1$. Now, we have $x \in \mathbb{Q}_p$ which is a field and so $\exists y \in \mathbb{Q}_p$ such that $xy = 1$. Then, $1 = |1|_p = |xy|_p = |x|_p|y|_p = 1.|y|_p = |y|_p$ and so $|y|_p = 1 \leq 1$. This implies that $y \in \mathbb{Z}_p$, hence x is a unit in $\mathbb{Z}_p$. □

Lemma 2.2.5. *Any nonzero element $x \in \mathbb{Z}_p$ can be written as $x = p^d y$, where $y \in \mathbb{Z}_p^{\times}$, and d is a non-negative integer.*

Proof. Let x be a nonzero element of $\mathbb{Z}_p$. Then, $x = \sum_{i=0}^{\infty} a_i p^i$, where $a_i \in \{0, 1, 2, ..., p-1\}$. Let d be the least non-negative integer such that $a_d \neq 0$ (such a number exists as $x \neq 0$). Then, $x = p^d(a_d + ad + 1p + ...)$. Now, as $a_d \neq 0$, we have $x \in \mathbb{Z}_p^{\times}$ which completes the proof. □

Lemma 2.2.6. *We have the inclusion*

$$\mathbb{Z}_p \supseteq p\mathbb{Z}_p \supseteq p^2\mathbb{Z}_p.... \ .$$

Proof. We have to show that $p^{k_1}\mathbb{Z}_p \subseteq p^{k_2}\mathbb{Z}_p$ whenever $k_1 \geq k_2$ are nonnegative integers. Let $x \in p^{k_1}\mathbb{Z}_p$, then, $x = p^{k_1}a$ where $a \in \mathbb{Z}_p$. Hence, $x = p^{k_2}p^{k_1-k_2}a$, where $p^{k_1-k_2}a \in \mathbb{Z}_p$(since $k_1 \geq k_2$ and $a \in \mathbb{Z}_p$) which completes the proof. □

Lemma 2.2.7. *Let I be an ideal of $\mathbb{Z}_p$. Then*

$$I = p^d\mathbb{Z}_p,$$

where d is a nonnegative integer.

Proof. Let I be an ideal of $\mathbb{Z}_p$. By lemma 2.2.5, for each nonzero element x of I, x can be written as $x = p^d y$, where $y \in \mathbb{Z}_p^\times$, and d is a non-negative integer. Let $a = p^d b$, where b is a unit, be an element of I with the minimum non-negative integer d. Now, as I is an ideal and b is a unit, we have

$$I \supseteq a\mathbb{Z}_p = p^d b\mathbb{Z}_p = p^d\mathbb{Z}_p,$$

Conversely, let $y \in I$, then, $y = p^l c$, where $l \geq d$ and c is a unit. Then, by previous lemma, we have $y = p^l c \in p^l\mathbb{Z}_p \subseteq p^d\mathbb{Z}_p$. Hence, $y \in p^d\mathbb{Z}_p$ which completes the proof. □

Corollary 2.2.8. *The unique maximal ideal in $\mathbb{Z}_p$ is $\pi = p.\mathbb{Z}_p$.*

Proof. As any ideal I in $\mathbb{Z}_p$ is of the form $I = p^d\mathbb{Z}_p$, and as we have the inclusion $\mathbb{Z}_p \supseteq p\mathbb{Z}_p \supseteq p^2\mathbb{Z}_p...$, one can easily see that the unique maximal ideal is $\pi = p.\mathbb{Z}_p$. □

Remark. We have

$$\mathbb{Z}_p = \mathbb{Z}_p^\times \bigcup p\mathbb{Z}_p.$$

Example 2.2.1. Fix a prime p. Then $\frac{1}{1-p}$ is an element of $\mathbb{Z}_p$. Note that

$$\frac{1}{1-p} = 1 + p + p^2 + ... \ .$$

Hence, $\frac{1}{1-p}$, is an element of $\mathbb{Z}_p$.

Example 2.2.2. Fix a prime p. Then -1 is an element of $\mathbb{Z}_p$. Note that

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + ... \ .$$

Therefore -1 is an element of $\mathbb{Z}_p$.

2.3 TOPOLOGY OF $\mathbb{Q}_P$

As a field with an absolute value forms a metric space, we can talk about the topology of this field. Particularly, we have an absolute value on the field $\mathbb{Q}_p$, and then we can consider the topological properties for $\mathbb{Q}_p$. In particular, the open balls in $\mathbb{Q}_p$ are defined to be:

$$B_\epsilon(a) = \{x \in \mathbb{Q}_p : |x - a| < \epsilon\}.$$

Similarly, the closed balls are defined to be:

$$\overline{B}_\epsilon(a) = \{x \in \mathbb{Q}_p : |x - a| < \epsilon\}.$$

The material in this section is taken from [2].

Remark. As we have $|x-y|_p = p^k$ provided $x, y \in \mathbb{Q}_p$, then, it is enough to consider these balls of the form $B_{p^k}(a)$, where $k \in \mathbb{Z}$, $a \in \mathbb{Q}_p$.

Lemma 2.3.1. *Let $\mathbb{Q}_p$ be the field of p-adic fractions, and let $\beta = \{B_{P^k}(x) : x \in \mathbb{Q}_p$ and $k \in \mathbb{Z}\}$ be the collection of all balls in $\mathbb{Q}_p$ then:*

(1) If $b \in B_{p^k}(a)$ then $B_{p^k}(a) = B_{p^k}(b)$,

(2) All the balls in β are open and closed at the same time,

(3) Two elements in the collection β intersect if and only if one of them contains the other.

Proof. (1) If $b \in B_{p^k}(a)$ then $|a - b|_p < p^k$. Let $x \in B_{p^k}(a)$, hence $|x - a|_p < p^k$. Now

$$|x - b|_p = |x - a + a - b|_p \leq \max(|x - a|_p, |a - b|_p) < p^k,$$

therefore $x \in B_{p^k}(b)$. For the other inclusion, let $x \in B_{p^k}(b)$, hence $|x - b|_p < p^k$. Which implies that

$$|x - a|_p = |x - b + b - a|_p \leq \max(|x - b|_p, |b - a|_p) < p^k,$$

and so $x \in B_{p^k}(a)$.

(2) This actually comes from the fact that the absolute value on $\mathbb{Q}_p$ takes discrete values, in other words, if $x \in \mathbb{Q}_p$ such that $|x|_p < p^k$, then $|x|_p \leq p^{k-1}$. Now, $B_{p^k}(a) = \{x \in$

$\mathbb{Q}_p$ such that $|x-a|_p < p^k\} = \{x \in \mathbb{Q}_p$ such that $|x-a|_p \leq p^{k-1}\}$.

(3) Let $B_{p^{k_1}}(a) \bigcap B_{p^{k_2}}(b) \neq \emptyset$. In other words, $\exists c \in B_{p^{k_1}}(a) \bigcap B_{p^{k_2}}(b)$. Without loss of generality, assume that $k_1 \geq k_2$, then by (1) we have

$$B_{p^{k_1}}(a) = B_{p^{k_1}}(c),$$

and

$$B_{p^{k_2}}(b) = B_{p^{k_2}}(c),$$

hence,

$$B_{p^{k_2}}(a) = B_{p^{k_2}}(c) \subseteq B_{p^{k_1}}(c) = B_{p^{k_1}}(b).$$

The other inclusion is obvious as if there is two non-empty set such that one of them contains the other then they do intersect. □

Now, lets consider the collection

$$\beta = \{B_{p^{-n}}(x) \text{ such that } x \in \mathbb{Q}_p \text{ and } n \in \mathbb{N}\},$$

we claim that this collection is a actually a basis for a topology on the field $\mathbb{Q}_p$, and that is obvious, since

(1) $\forall x \in \mathbb{Q}_p$ we have $x \in B_{p^{-n}}(x) \, \forall \, n \in \mathbb{N}$,

(2) If $x \in B_{p^{-n_1}}(y) \bigcap B_{p^{-n_2}}(z)$ then by previous lemma we have

$$B_{p^{-n_1}}(y) = B_{p^{-n_1}}(x)$$

and

$$B_{p^{-n_2}}(z) = B_{p^{-n_2}}(x).$$

Now, take $n \geq \max(n_1, n_2)$, then

$$x \in B_{p^{-n}}(x) \subseteq B_{p^{-n_1}}(x) \bigcap B_{p^{-n_2}}(x) = B_{p^{-n_1}}(y) \bigcap B_{p^{-n_2}}(z).$$

The topology on $\mathbb{Q}_p$ is the topology induced by this basis, and so the set U is open in $\mathbb{Q}_p$ if and only if U is equal to a union of some elements in β.

Lemma 2.3.2. *Let a be an element of $\mathbb{Q}_p$ and $n \in \mathbb{N}$, then*

$$B_{p^{(1-n)}}(a) = a + p^n\mathbb{Z}_p.$$

Proof. $x \in a + p^n\mathbb{Z}_p \iff x - a \in p^n\mathbb{Z}_p$

$\iff |x - a|_p \leq p^{-n}$

$\iff |x - a|_p < p^{-n+1}$

$\iff x \in B_{p^{(-n+1)}}(a)$.

Hence,

$$B_{p^{(1-n)}}(a) = a + p^n\mathbb{Z}_p.$$

□

Lemma 2.3.3. *The ball $B_{p^{(1-n)}}(1) = 1 + p^n\mathbb{Z}_p$ is a subgroup of $\mathbb{Z}_p$.*

Proof. Let's first prove that $1 + p^n\mathbb{Z}_p$ is closed under multiplication. Let $x, y \in 1 + p^n\mathbb{Z}_p$, which implies that $x = 1 + p^n m_1$ and $y = 1 + p^n m_2$, where $m_1, m_2 \in \mathbb{Z}_p$. Then,

$$\begin{aligned} xy &= 1 + p^n(m_1 + m_2) + p^n p^n m_1 m_2 \\ &= 1 + p^n(m_1 + m_2 + p^n m_1 m_2) \end{aligned}$$

where $m_1 + m_2 + p^n m_1 m_2$ is in $\mathbb{Z}_p$ (since each single term is, and $\mathbb{Z}_p$ is an integral domain). Now, let $z = m_1 + m_2 + p^n m_1 m_2$, then

$$xy = 1 + p^n z,$$

where $z \in \mathbb{Z}_p$. Therefore, $xy \in 1 + p^n\mathbb{Z}_p$. Now, $w \in 1 + p^n\mathbb{Z}_p$ if and only if $w = 1 + p^n m$, where $m \in \mathbb{Z}_p$ if and only if

$$\begin{aligned} \frac{1}{w} &= \frac{1}{1+p^n m} \\ &= \frac{1+p^n m - p^n m}{1+p^n m} \\ &= 1 + \frac{p^n(-m)}{1+p^n m} \ . \end{aligned}$$

We want to show that $\frac{-m}{1+p^n m} \in \mathbb{Z}_p$. We have $|\frac{-m}{1+p^n}|_p = |-m|_p|\frac{1}{1+p^n m}|_p$, but $|\frac{1}{1+p^n m}|_p = 1$ as $|1 + p^n m| = 1$. Hence, $|\frac{-m}{1+p^n m}|_p = |-m|_p = |m|_p \leq 1$ as $m \in \mathbb{Z}_p$. Therefore, $\frac{-m}{1+p^n m} \in \mathbb{Z}_p$ which implies that $1 + p^n \frac{-m}{1+p^n m} \in \mathbb{Z}_p$. Thus, $w^{-1} \in \mathbb{Z}_p$. □

CHAPTER 3

ACTION OF $GL(2, \mathbb{Q}_P)$ ON $V(\chi_1, \chi_2)$

3.1 CHARACTERS OF $\mathbb{Q}_P^\times$

Definition. Let G be a topological group, then a quasi character is a continuous homomorphism from G to $\mathbb{C}^\times$.

Definition. Let G be a topological group, then a character is a continuous homomorphism from G to $S^1 = \{z \in \mathbb{C} \text{such that} |z|_c = 1\}$.

Remark. Given $z = a + bi \in \mathbb{C}$, then $|z|_c$ is defined by

$$|z|_c := \sqrt{a^2 + b^2}.$$

Theorem 3.1.1. *Let $\mu : \mathbb{Q}_p^\times \to \mathbb{C}$ be a quasi character, then $\exists\, n \in \mathbb{N}$ such that*

$$\mu\left(1 + p^n \mathbb{Z}_p\right) = 1.$$

Proof. First note that $\mu(1) \neq 0$ since $\mu(1) \in \mathbb{C}^\times$. Now, we have $\mu(1) = \mu(1.1) = \mu(1)\mu(1)$ and so $\mu(1) = 1$. Now, $\mu(1) = 1$ and μ is continuous (since it is a quasi character). Let V be a neighborhood of 1, then by the continuity of μ, there exists an open set U containing 1 such that $\mu(U) \subseteq V \subseteq \mathbb{C}^\times$. Now, since U is open, we have $U = \bigcup_{i \in I} B_{p^{-n_i}}(a_i)$ for some $n_i's \in \mathbb{N}$ and $a_i's \in \mathbb{Q}_p^\times$, and as $1 \in U$, then $1 \in B_{p^{1-n_i}}(a_i) \subseteq U$ for some $i \in I$. By lemma 2.3.1 , we know that since $1 \in B_{p^{1-n_i}}(a)$, then

$$B_{p^{1-n_i}}(1) = B_{p^{1-n_i}}(a).$$

Now, we know by previous lemma that $B_{p^{1-n_i}}(1)$ is a subgroup and we know that μ is a homomorphism. Hence, $\mu\left(B_{p^{1-n_i}}(1)\right) \subseteq V$ is a subgroup as well. Assume for the sake of contradiction that there is some $u \in \mu\left(B_{p^{1-n_i}}(1)\right)$ such that $u \neq 1$. We can choose the open set V to be very small from the beginning so that some powers of any nontrivial element

in V will go out of V, which contradicts the fact that $\mu\left(B_{p^{1-n_i}}(1)\right)$ is a subgroup. Hence, $\mu\left(B_{p^{1-n_i}}(1)\right) = 1$. But

$$B_{p^{(1-n_i)}}(1) = 1 + p^{n_i}\mathbb{Z}_p,$$

and so

$$\mu\left(1 + p^{n_i}\mathbb{Z}_p\right) = 1.$$

□

Remark. From lemma 2.2.6, we have

$$\mathbb{Z}_p \supseteq p\mathbb{Z}_p \supseteq p^2\mathbb{Z}_p \ldots\ ,$$

and hence

$$1 + \mathbb{Z}_p \supseteq 1 + p\mathbb{Z}_p \supseteq 1 + p^2\mathbb{Z}_p \ldots\ ,$$

so, it is reasonable to define the least integer $n \in \mathbb{N}$ such that

$$\mu(1 + p^n\mathbb{Z}_p) = 1.$$

Let's first note that $1 + \mathbb{Z}_p = \mathbb{Z}_p$. Then, if $\mu|_{(\mathbb{Z}_p - \{0\})}$ is trivial then $\mu(p^n) = 1$ for all positive integers n. Now, if $x \in \mathbb{Q}_p^\times$ then $|x|_p = p^k$ where $k \in \mathbb{Z}$. Let $m > |k|$, then p^m and $y := p^m x$ are elements of $\mathbb{Z}_p$. Then we have $1 = \mu(y) = \mu(p^m x) = \mu(p^m)\mu(x) = 1.\mu(x) = \mu(x)$. Hence, if $\mu|_{(\mathbb{Z}_p - \{0\})} = 1$ then μ is trivial.

Definition. Let μ be a quasi character. Then the conductor of μ, denoted by $cond(\mu)$ is defined to be zero if $\mu|_{\mathbb{Z}_p^\times}$ is trivial. Otherwise, it is defined to be the least element $n \in \mathbb{N}$ such that

$$\mu(1 + p^n\mathbb{Z}_p) = 1.$$

Corollary 3.1.2. *Let μ_1, μ_2 be quasi characters. Then there exists $n \in \mathbb{N}$ such that*

$$\mu_1(1 + p^n\mathbb{Z}_p) = \mu_2(1 + p^n\mathbb{Z}_p) = 1.$$

Proof. First, if μ_1, μ_2 are both trivial on $\mathbb{Z}_p^\times$ then $\forall\, n \in \mathbb{N}$ we have

$$\mu_1(1+p^n\mathbb{Z}_p) = \mu_2(1+p^n\mathbb{Z}_p) = 1.$$

Now assume that one of the quasi characters is non-trivial on $\mathbb{Z}_p^\times$ and the other is trivial on $\mathbb{Z}_p^\times$, say $\mu_1|_{\mathbb{Z}_p^\times} \neq 1$ but $\mu_1|_{\mathbb{Z}_p^\times} = 1$. Let $n_1 \in \mathbb{N}$ denote the conductor of μ_1, then $\mu_1|_{1+p^{n_1}\mathbb{Z}_p} = 1$ and as $1+p^{n_1}\mathbb{Z}_p \subseteq \mathbb{Z}_p^\times$ then $\mu_2|_{1+p^{n_1}\mathbb{Z}_p} = 1$. Hence Let μ_1, μ_2 be quasi characters. Then there exists $n \in \mathbb{N}$ such that

$$\mu_1(1+p^{n_1}\mathbb{Z}_p) = \mu_2(1+p^{n_1}\mathbb{Z}_p) = 1.$$

Now assume that both of the quasi characters μ_1, μ_2 are non-trivial on $\mathbb{Z}_p^\times$ and let n_1, n_2 be the conductors of μ_1, μ_2 respectively. Then $\mu_1(1+p^{n_1}\mathbb{Z}_p) = 1$ and $\mu_2(1+p^{n_2}\mathbb{Z}_p) = 1$. Choose $n = \max(n_1, n_2)$. Therefore, by lemma 2.2.6, we have

$$1+p^n\mathbb{Z}_p \subseteq 1+p^{n_1}\mathbb{Z}_p,$$

and

$$1+p^n\mathbb{Z}_p \subseteq 1+p^{n_2}\mathbb{Z}_p.$$

Hence $\mu_1(1+p^n\mathbb{Z}_p) = \chi_1(1+p^{n_1}\mathbb{Z}_p)$=1, and $\mu_2(1+p^n\mathbb{Z}_p) = \mu_2(1+p^{n_2}\mathbb{Z}_p) = 1$. □

3.2 STUDY OF $GL(2,\mathbb{Q}_P)$ AND ITS TOPOLOGY

As we have a topology on $\mathbb{Q}_p$, We can define a topology on the set $GL(2,\mathbb{Q}_p)$ which is the set of all invertible matrices over $\mathbb{Q}_p$. Indeed, the topology of $GL(2,\mathbb{Q}_p)$ will be very similar to the one of $\mathbb{Q}_p$, in other words, $GL(2,\mathbb{Q}_p)$ will *inherit* the structure of the topological group $\mathbb{Q}_p$. And then, most of the topological properties that we have in $\mathbb{Q}_p$, will be satisfied on $GL(2,\mathbb{Q}_p)$.

Definition. Let R be a commutative ring with unity, then we define

$GL(2,R)$ to be the set of all elements $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $a,b,c,d \in R$, such that there exists a 2×2 matrix B with entries from R satisfying $AB = I$.

Definition. Let R be a commutative ring with unity and let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be a matrix over R. Then, the determinant of A is defined to be

$$det(A) = ad - bc.$$

Lemma 3.2.1. *Let R be a commutative ring with unity and let A, B be any 2×2 matrices over a R, then*

$$det(AB) = det(A)det(B).$$

Proof. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$. Then, $AB = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}$. Hence, $det(AB) = (ae+bg)(cf+dh) - (ce+dg)(af+bh) = aecf + aedh + bgcf + bgdh - afce - afdg - bhce - bhdg = ad(eh-fg) - cb(eh-fg) = (eh-fg)(ad-cb) = det(A)det(B)$. □

Lemma 3.2.2. *Let R be a commutative ring with unity, then*

$$GL(2,R) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ with } a,b,c,d \in R \text{ and } ad-bc \in R^{\times} \right\}.$$

Proof. Suppose that $A \in GL(2, \mathbb{Q}_p)$, then by definition, $\exists$ a 2×2 matrix B over R such that $AB = I$. Now, from the previous lemma we have $det(A)det(B) = det(I) = 1$. Hence, $det(A)$, $det(B)$ are both units.

Conversely, let $A \in \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ with } a,b,c,d \in R \text{ and } ad-bc \in R^{\times} \right\}$. First we show that $\frac{a}{ad-cb}, \frac{b}{ad-cb}, \frac{c}{ad-cb}, \frac{d}{ad-cb} \in R$. Now, since $ad - cb \in R^{\times}$, we have $\frac{1}{ad-cb} \in R$ and since R is a ring, each of $\frac{a}{ad-cb}, \frac{b}{ad-cb}, \frac{c}{ad-cb}, \frac{d}{ad-cb} \in R$. Now, it is easy to check that the matrix

$B = \begin{bmatrix} \frac{d}{ad-cb} & -\frac{b}{ad-cb} \\ -\frac{c}{ad-cb} & \frac{a}{ad-cb} \end{bmatrix}$ satisfies $AB = I$. This implies that $A \in GL(2, R)$. Hence,

$$\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ with } a, b, c, d \in R \text{ and } ad - bc \in R^{\times} \right\} \subseteq GL(2, R).$$

Then, we conclude that

$$GL(2, R) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ with } a, b, c, d \in R \,\text{and}\, ad - bc \in R^{\times} \right\}.$$

□

Remark. In particular, we have

$$GL(2, \mathbb{Z}_p) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \textit{ such that } a, b, c, d \in \mathbb{Z}_p \textit{ and } ad - cb \in \mathbb{Z}_p^{\times} \right\},$$

and we have

$$GL(2, \mathbb{Q}_p) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \textit{ such that } a, b, c, d \in \mathbb{Q}_p \textit{ and } ad - cb \in \mathbb{Q}_p^{\times} \textit{ or } ad - cb \neq 0 \right\}.$$

Lets now define some sets that are important for our work:

$$(1)\ B(\mathbb{Q}_p) = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \text{ such that } a, d \in \mathbb{Q}_p^{\times}, b \in \mathbb{Q}_p \right\}$$

$$(2)\ K(p^n) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ such that } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv I \bmod(p^n) \right\}$$

$$(3)\ B(\mathbb{Z}_p) = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \text{ such that } a, d \in \mathbb{Z}_p^{\times}, b \in \mathbb{Z}_p \right\}$$

It is easy to check that all the previous subsets are actually subgroups of $GL(2, \mathbb{Q}_p)$.

Now, we want to define a metric d on

$$GL(2, \mathbb{Q}_p) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ with } a, b, c, d \in R \text{ and } ad - bc \in R^{\times} \right\}.$$

Define $d : GL(2, \mathbb{Q}_p) \times GL(2, \mathbb{Q}_p) \to \mathbb{R}$ by the following :

$$d\left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \right) = \max(|a_1 - a_2|_p, |b_1 - b_2|_p, |c_1 - c_2|_p, |d_1 - d_2|_p).$$

Let $x = \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \in GL(2, \mathbb{Q}_p)$, then

$$\begin{aligned} B_\epsilon\left(\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}\right) &= \left\{ \begin{bmatrix} y_1 & y_2 \\ y_3 & y_4 \end{bmatrix} \in GL(2, \mathbb{Q}_p) \text{ such that } d(\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}, \begin{bmatrix} y_1 & y_2 \\ y_3 & y_4 \end{bmatrix}) < \epsilon \right\} \\ &= \left\{ \begin{bmatrix} y_1 & y_2 \\ y_3 & y_4 \end{bmatrix} \in GL(2, \mathbb{Q}_p) \text{ such that } \max_{1 \leq i \leq 4}(|x_i - y_i|_p) < \epsilon \right\} \\ &= \left\{ \begin{bmatrix} y_1 & y_2 \\ y_3 & y_4 \end{bmatrix} \in GL(2, \mathbb{Q}_p) \text{ such that } \forall\ 1 \leq i \leq 4 \ \ |x_i - y_i|_p < \epsilon \right\} \\ &= \left\{ \begin{bmatrix} y_1 & y_2 \\ y_3 & y_4 \end{bmatrix} \in GL(2, \mathbb{Q}_p) \text{ such that } \forall\ 1 \leq i \leq 4 \ \ y_i \in B_\epsilon(x_i) \right\} \end{aligned}$$

Now, since the only possible results from the absolute values are p^k for some $k \in \mathbb{Z}$. It is enough to consider the balls $B_{p^k}\left(\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}\right)$ such that $k \in \mathbb{Z}$. Furthermore, it is easy to check that the collection

$$\beta = \left\{ B_{p^{-n}}\left(\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}\right) \text{ such that } n \in \mathbb{N} \textit{ and } \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \in GL(2, \mathbb{Q}_p) \right\},$$

is a basis and then, the topology on $GL(2, \mathbb{Q}_p)$ is the topology generated by these basis, i.e., the set $U \subseteq GL(2, \mathbb{Q}_p)$ is open if and only if it can be written as union of elements from β.

Lemma 3.2.3. *Let $n \in \mathbb{N}$, then*

$$B_{p^{1-n}}(I_2) = K(p^n).$$

Proof.

$$\begin{aligned}
K(p^n) &= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2,\mathbb{Z}_p) \text{ such that } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv I_2 \bmod(p^n) \right\} \\
&= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2,\mathbb{Z}_p) \text{ such that } \begin{array}{c} a-1 = k_1 p^n \, , d-1 = k_2 p^n, \, c = k_4 p^n, \\ b = k_3 p^n \text{ where } k_i \in \mathbb{Z}_p \end{array} \right\} \\
&= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2,\mathbb{Z}_p) \text{ such that } |a-1|_p, \, |d-1|_p \leq p^{-n}, \, |b|_p, \, |c|_p \leq p^{-n} \right\} \\
&= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2,\mathbb{Z}_p) \text{ such that } |a-1|_p, \, |d-1|_p < p^{1-n}, \, |b|_p, \, |c|_p < p^{1-n} \right\} \\
&= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2,\mathbb{Z}_p) \text{ such that } a, d \in B_{p^{1-n}}(1) \;\; b, c \in B_{p^{1-n}}(0) \right\} \\
&= B_{p^{1-n}}(I_2).
\end{aligned}$$

□

After this lemma, it is easy for us to see the relation between the sets $K(p^n)$'s for different n's$\in \mathbb{N}$ which is

$$K(p) \supset K(p^2) \supset K(p^3) \supset .... \; .$$

Remark. Notice that

$$\overline{B_{p^{-n}}(I_2)} = B_{p^{1-n}}(I_2) = K(p^n).$$

Lemma 3.2.4. *Let $n \in \mathbb{N}$ and let A, B be in $GL(2, \mathbb{Q}_p)$ such that $B \in B_{p^{-n}}(A)$, then*

$$B_{p^{-n}}(B) = B_{p^{-n}}(A).$$

Proof. Let $A = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}$, $B = \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}$ be two matrices in $GL(2, \mathbb{Q}_p)$. Then, we have

$$B_{p^{-n}}\left(\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}\right) = \left\{ \begin{bmatrix} y_1 & y_2 \\ y_3 & y_4 \end{bmatrix} \in GL(2, \mathbb{Q}_p) \text{ such that } y_i \in B_{p^{-n}}(a_i) \ \forall \ 1 \leq i \leq 4 \right\}.$$

Now, since $\begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} \in B_{p^{-n}}\left(\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}\right)$, then we have $b_i \in B_{p^{-n}}(a_i)$ $\forall 1 \leq i \leq 4$.
Now, by lemma 2.3.1, we conclude that

$$B_{p^{-n}}(b_i) = B_{p^{-n}}(a_i).$$

Therefore,

$$\begin{aligned} B_{p^{-n}}\left(\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}\right) &= \left\{ \begin{bmatrix} y_1 & y_2 \\ y_3 & y_4 \end{bmatrix} \in GL(2, \mathbb{Q}_p) \text{ such that } y_i \in B_{p^{-n}}(b_i) \ \forall \ 1 \leq i \leq 4 \right\} \\ &= B_{p^{-n}}\left(\begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}\right). \end{aligned}$$

□

Lemma 3.2.5. *The set $GL(2, \mathbb{Q}_p)$ is a topological group with respect to the topology τ' generated by the basis*

$$\beta = \left\{ B_{p^{-n}}(\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}) \text{ such that } n \in \mathbb{N} \text{ and } \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \in GL(2, \mathbb{Q}_p) \right\}.$$

Proof. See some reference. □

Lemma 3.2.6. *For each open set U containing $g \in GL(2, \mathbb{Q}_p)$, U contains $gK(p^n)$ for some $n \in \mathbb{N}$.*

Proof. Since the set $GL(2, \mathbb{Q}_p)$ is a topological group, then the function

$$f : GL(2, \mathbb{Q}_p) \times GL(2, \mathbb{Q}_p) \to GL(2, \mathbb{Q}_p),$$

by

$$f(g_1, g_2) = g_1 g_2,$$

is continuous. Note that $f(g, I) = g$, and so if U is an open set containing g then $\exists\ U_1,\ U_2$ open sets containing g, I respectively such that $f(U_1, U_2) \subseteq U$ or equivalently $U_1 U_2 \subseteq U$. Now, U_2 is a union of some balls of the form $B_{p^{-n}}(a)$ for some $n's \in \mathbb{N}$ and $a's \in GL(2, \mathbb{Q}_p)$. Since $I \in U_2$ then $I \in B_{p^{-n}}(a)$ for some $n \in \mathbb{N}$ and $a \in GL(2, \mathbb{Q}_p)$. Hence, by lemma 3.2.4, we have

$$B_{p^{-n}}(I) = B_{p^{-n}}(a).$$

Now, we have $B_{p^{-n}}(I) \subseteq U_2$ and $g \in U_1$, therefore $gB_{p^{-n}}(I) \subseteq U_1 U_2 = U$. But by lemma 3.2.3, we know that

$$B_{p^{-n}}(I) = B_{p^{1-(n+1)}}(I) = K(p^{n+1}),$$

therefore $gK(p^{n+1}) \subseteq U$. □

Lemma 3.2.7. *The collection*

$$\beta' = \{g(Kp^m) \text{ such that } g \in GL(2, \mathbb{Q}_p) \text{ and } m \in \mathbb{N}\},$$

is actually a basis.

Proof. (1) Suppose that $g \in GL(2, \mathbb{Q}_p)$, then obviously, g is contained in $gK(p^m)\ \forall m \in \mathbb{N}$. (2) Assume $g \in g_1 K(p^m) \bigcap g_2 K(p^n)$. Without loss of generality, assume that $m \geq n$, then,

since $K(p^m)$ and $K(p^n)$ are subgroups, we have:

$$gK(p^m) = g_1K(p^m),$$

and

$$gK(p^n) = g_2K(p^n),$$

and hence

$$gK(p^m) \subset gK(p^m) \bigcap gK(p^n) = g_1K(p^m) \bigcap g_2K(p^n).$$

□

We now have two different topologies on the topological group $GL(2, \mathbb{Q}_p)$ the one generated by

$$\beta^{'} = \{gK(p^m) \text{ such that } g \in GL(2, \mathbb{Q}_p) \text{ and } m \in \mathbb{N}\},$$

and the one generated by

$$\beta = \left\{ B_{p^{-n}} \left(\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \right) \text{ such that } n \in \mathbb{N} \text{ and } \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \in GL(2, \mathbb{Q}_p \right\}.$$

Then it is rational to ask whether these two topologies comparable, and if yes, whether either of them finer than the other or they are the same. The following lemma will actually answer this question.

Lemma 3.2.8. *The topology $\tau^{'}$ generated by the basis $\beta^{'} = \{gK(p^m)$ such that $g \in GL(2, \mathbb{Q}_p)$ and $m \in \mathbb{N}\}$ and the topology τ generated by the basis $\beta = \left\{ B_{p^{-n}} \left(\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \right) \text{ such that } n \in \mathbb{N} \text{ and } \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \in GL(2, \mathbb{Q}_p \right\}$ are actually the same.*

Proof. Let $U \in \tau$, then U is a union of some balls of the form $B_{p^{-n}}(x)$ for some $x's \in GL(2, \mathbb{Q}_p)$ and some $n's \in \mathbb{N}$. But each of $B_{p^{-n}}(x)$ is a $\tau-$open set. Now, according to lemma 3.2.7, for each $g \in B_{p^{-n}}(x)$, $B_{p^{-n}}(x)$ contains $gK(p^{m_g})$ for some $m_g \in \mathbb{N}$. Hence,

$B_{p^{-n}}(x) = \bigcup_{g \in B_{p^{-n}}(x)} gK(p^k)$ for some $k's \in \mathbb{N}$. Since this is true for all the balls where U is written as union of, then U itself is a union of some elements of the form $gK(p^m)$ for all $g's \in U$ and some $m's \in \mathbb{N}$. Therefore, U is a $\tau^{'}-$open set, or, $U \in \tau^{'}$.

Conversely, let $gK(p^n) \in \beta^{'}$. Now, as $g \in GL(2, \mathbb{Q}_p)$ $\exists g^{-1} \in GL(2, \mathbb{Q}_p)$ such that $g^{-1}g = I$. Now, as $K(p^n) \in \beta^{'}$, then it is open. We know that $I \in K(p^n)$. As by lemma (3.2.5) we have that $GL(2, \mathbb{Q}_p)$ is a topological group with respect to the topology τ generated by the basis $\beta = \left\{ B_{p^{-n}} \left(\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \right) \text{ such that } n \in \mathbb{N} \text{ and } \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \in GL(2, \mathbb{Q}_p \right\}$, then the multiplication is continuous, and so there exists two $\tau-$open sets U, V containing g, g^{-1} respectively such that $VU \in K(p^n)$. Now, as $g^{-1} \in V$, we have $g^{-1}U \subseteq K(p^n)$. This implies that $U \subseteq gK(p^n)$. Now, as $K(p^n)$ is subgroup, then we have $h \in gK(p^n)$ if and only if $hK(p^n) = gK(p^n)$. Hence, for each $h \in gK(p^n)$, we have an open set W containing h such that $W \subseteq gK(p^n)$. This implies that $gK(p^n)$ can be written as union of τ-open sets (sets that are open in the topology τ), hence $gK(p^n)$ is open in τ, i.e., $gK(p^n) \in \tau$. Now, as every $U^{'} \in \tau^{'}$ is a union of elements of the form $gK(p^n)$, then we have $U^{'} \in \tau$. $\square$

3.3 LOCALLY CONSTANT FUNCTIONS FROM $GL(2,\mathbb{Q}_P)$ TO $\mathbb{C}$

Definition. A function $f : GL(2,\mathbb{Q}_p) \to \mathbb{C}$ is locally constant if $\forall g \in GL(2,\mathbb{Q}_p)$ $\exists$ an open set U containing g such that:

$$f(u) = f(g) \quad \forall u \in U.$$

Lemma 3.3.1. *A function $f : GL(2,\mathbb{Q}_p) \to \mathbb{C}$ is locally constant if and only if $\forall g \in GL(2,\mathbb{Q}_p)$ $\exists n \in \mathbb{N}$ such that $f|_{gK(p^n)}$ is constant.*

Proof. Suppose $f : GL(2,\mathbb{Q}_p) \to \mathbb{C}$ is locally constant. Let $g \in GL(2,\mathbb{Q}_p)$, then $\exists$ an open set U such that $g \in U$ and $f(u) = f(g)$ $\forall u \in U$. Now, by lemma 3.2.6, we have that $\exists$ $n \in \mathbb{N}$ such that $gK(p^n) \subseteq U$. Therefore, f is constant on $gK(p^n)$.

Conversely, suppose $\forall g \in GL(2,\mathbb{Q}_p)$ $\exists$ $n \in \mathbb{N}$ such that $f|_{gK(p^n)}$ is constant. Now, the set $gK(p^n)$ is open itself. Therefore, take $U := gK(p^n)$, then $f|_U$ is constant and hence f is locally constant. □

Lemma 3.3.2. *The subgroup $K(p^n)$ is normal in $\mathbb{Z}_p$.*

Proof. Consider $f : GL(2,\mathbb{Z}_p) \to GL(2,\mathbb{Z}_p/p^n\mathbb{Z}_p)$ defined by the following

$$f\left(\begin{bmatrix} \sum_{i=0}^{\infty} a_i p^i & \sum_{i=0}^{\infty} b_i p^i \\ \sum_{i=0}^{\infty} c_i p^i & \sum_{i=0}^{\infty} d_i p^i \end{bmatrix}\right) = \begin{bmatrix} \sum_{i=0}^{n} a_i p^i & \sum_{i=0}^{n} b_i p^i \\ \sum_{i=0}^{n} c_i p^i & \sum_{i=0}^{n} d_i p^i \end{bmatrix}.$$

Now, let $g = \begin{bmatrix} g_1 & g_2 \\ g_3 & g_4 \end{bmatrix} \in GL(2,\mathbb{Z}_p)$, then $f\left(\begin{bmatrix} g_1 & g_2 \\ g_3 & g_4 \end{bmatrix}\right) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ if and only if

$$g_1, g_4 \equiv 1 \bmod(p^n),$$

and

$$g_2, g_3 \equiv 0 \bmod(p^n),$$

if and only if

$$g = \begin{bmatrix} g_1 & g_2 \\ g_3 & g_4 \end{bmatrix} \in K(p^n),$$

therefore

$$ker(f) = K(p^n),$$

and so $K(p^n)$ is normal in $GL(2, \mathbb{Z}_p)$. □

Lemma 3.3.3. *The group $GL(2, \mathbb{Z}_p)$ is compact.*

Proof. See [4]. □

Theorem 3.3.4. *Let $f : GL(2, \mathbb{Z}_p) \to \mathbb{C}$ be a locally constant function then $\exists\ n \in \mathbb{N}$ such that $f|_{gK(p^n)}$ is constant for all $g \in GL(2, \mathbb{Z}_p)$.*

Proof. Suppose that $f : GL(2, \mathbb{Z}_p) \to \mathbb{C}$ is a locally constant function, then by lemma 3.3.1, $\forall\, g \in GL(2, \mathbb{Z}_p)\ \exists\ n \in \mathbb{N}$ such that $f|_{gK(p^n)}$ is constant. Now, as we have the inclusion

$$K(p) \supseteq K(p^2) \supseteq K(p^3) ... \ ,$$

then the n we for each g is not unique (for example if you get an m such that $f|_{gK(p^m)}$ is constant then $\forall k \geq m$ we have $f|_{gK(p^k)}$ is constant). Hence, given $g \in GL(2, \mathbb{Z}_p)$, let

$$m = \min\{n \in \mathbb{N} \text{ such that } f|_{gK(p^n)} \text{is constant}\}.$$

Now, do the same thing for each $g \in GL(2, \mathbb{Z}_p)$ and then consider the collection of sets $\beta = \{gK(p^m) \text{ such that } g \in GL(2, \mathbb{Z}_p) \text{ and } m \text{ is that minimum } m \text{ such that } f|_{gK(p^m)} \text{is constant}\}$. Now, obviously, this collection is a cover of $GL(2, \mathbb{Z}_p)$ and since $GL(2, \mathbb{Z}_p)$ is compact, there should be a finite sub-cover, say

$$g_1K(p^{m_1}), g_2K(p^{m_2}), ..., g_lK(p^{m_l}).$$

Now, assume without loss of generality that

$$m_1 = \max\{m_1, m_2, ..., m_l\},$$

then for each $i = 1, 2, ..., l$ the function f restricted on the coset $g_iK(p^{m_1})$ is equal to some constant c_i, hence

$$f|_{g_1K(p^{m_1})} = c_1,$$

$$f|_{g_2K(p^{m_1})} = c_2,$$

.

.

.

$$f|_{g_lK(p^{m_1})} = constant = c_l,$$

but

$$GL(2, \mathbb{Z}_p) = g_1K(p^{m_1}) \bigcup g_2K(p^{m_2}) ... \bigcup g_lK(p^{m_l}).$$

Now, if $g \in GL(2, \mathbb{Z}_p)$ then $g \in g_iK(p^{m_i})$ for some $i \in \{1, 2, ..., l\}$ and since $K(p^m)$ is a subgroup, we have $gK(p^{m_i}) = g_iK(p^{m_i})$ and then

$$gK(p^{m_1}) \subseteq gK(p^{m_i}) = g_iK(p^{m_i}),$$

and so

$$f|gK(p^{m_1}) = c_i.$$

□

3.4 IWASAWA'S THEOREM

Our main concern in this section is to understand and give a detailed proof of Iwasawa's theorem, which says that given an element $g \in GL(2, \mathbb{Q}_p)$, then g can be decomposed as, $g = bk$, such that $b \in B(\mathbb{Q}_p)$ and $k \in GL(2, \mathbb{Z}_p)$, where this decomposition is unique up to certain conditions. Now, in order to prove this theorem, we have to prove some lemmas first.

Lemma 3.4.1. *Given $u, v \in \mathbb{Z}_p$, then $\exists\, r, s \in \mathbb{Z}_p$ such that*

$$g = \begin{bmatrix} r & s \\ u & v \end{bmatrix} \in GL(2, \mathbb{Z}_p),$$

if and only if at least one of $u, v \in \mathbb{Z}_p$.

Proof. Suppose that $g = \begin{bmatrix} r & s \\ u & v \end{bmatrix} \in GL(2, \mathbb{Z}_p)$ which implies that $rv - us \in \mathbb{Z}_p^{\times}$, or equivalently $|rv - us|_p = 1$. Now, $1 = |rv - us|_p \leq \max(|rv|_p, |us|_p)$. Without loss of generality, assume that $\max(|rv|_p, |us|_p) = |rv|_p$, then we have $|rv|_p \geq 1$ or $|r|_p|v|_p \geq 1$. But $1 \geq |r|_p$ since $r \in \mathbb{Z}_p$. This implies that $|v|_p = 1.|v|_p \geq |r|_p|v|_p \geq 1$. Since we know that $v \in \mathbb{Z}_p$, we get $|v|_p \leq 1$, and so $|v|_p = 1$, which is equivalent to saying that $v \in \mathbb{Z}_p^{\times}$. Conversely, suppose (without loss of generality) that $v \in \mathbb{Z}_p^{\times}$ and $u \in \mathbb{Z}_p$. We should show that $\exists r, s \in \mathbb{Z}_p$ such that $\begin{bmatrix} r & s \\ u & v \end{bmatrix} \in GL(2, \mathbb{Z}_p)$.
As $u, v \in \mathbb{Z}_p$ and $v \in \mathbb{Z}_p^{\times}$, we have $v^{-1} \in \mathbb{Z}_p^{\times} \subseteq \mathbb{Z}_p$. Choose

$$\begin{aligned} r &:= v^{-1} + u, \text{ and} \\ s &:= v, \end{aligned}$$

then

$$\begin{aligned} rv - us &= (v^{-1} + u)v - uv \\ &= 1 + uv - uv \\ &= 1, \end{aligned}$$

and hence

$$|rv - us|_p = |1|_p = 1,$$

or

$$rv - us \in \mathbb{Z}_p^{\times},$$

and so $\begin{bmatrix} r & s \\ u & v \end{bmatrix} \in GL(2, \mathbb{Z}_p)$.

□

Lemma 3.4.2. *If* $g = \begin{bmatrix} g_1 & g_2 \\ g_3 & g_4 \end{bmatrix} \in GL(2, \mathbb{Q}_p)$ *then* $\exists\, k \in GL(2, \mathbb{Z}_p)$ *such that*

$$g = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} k,$$

for some $a, d \in \mathbb{Q}_p^{\times}$ *and* $b \in \mathbb{Q}_p$ *if and only if* $\exists\, k \in GL(2, \mathbb{Z}_p)$ *such that the bottom row is a scalar multiple of the bottom row of* g.

Proof. Suppose that $g = \begin{bmatrix} g_1 & g_2 \\ g_3 & g_4 \end{bmatrix} \in GL(2, \mathbb{Q}_p)$ and $k \in GL(2, \mathbb{Z}_p)$ such that

$$g = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} k,$$

with $a, d \in \mathbb{Q}_p^{\times}$ and $b \in \mathbb{Q}_p$. Now, we have $g = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix} = \begin{bmatrix} * & * \\ dk_3 & dk_4 \end{bmatrix}$

which implies that

$$(g_3 \;\; g_4) = (dk_3 \;\; dk_4)\,.$$

As $d \in \mathbb{Q}_p^{\times}$, we conclude that

$$(k_3 \;\; k_4) = \left(d^{-1}g_3 \;\; d^{-1}g_4\right).$$

Conversely, given $k \in GL(2,\mathbb{Z}_p)$ and $g \in GL(2,\mathbb{Q}_p)$ such that $g = \begin{bmatrix} g_1 & g_2 \\ g_3 & g_4 \end{bmatrix} \in GL(2,\mathbb{Q}_p)$ and $k = \begin{bmatrix} k_1 & k_2 \\ \alpha g_3 & \alpha g_4 \end{bmatrix} \in GL(2,\mathbb{Z}_p)$ where $\alpha \in \mathbb{Q}_p^{\times}$, then

$$k^{-1} = \begin{bmatrix} \frac{g_4}{k_1 g_4 - g_3 k_2} & \frac{-k_2}{\alpha(k_1 g_4 - k_2 g_3)} \\ \frac{-g_3}{k_1 g_4 - g_3 k_2} & \frac{k_1}{\alpha(k_1 g_4 - k_2 g_3)} \end{bmatrix},$$

which implies that

$$\begin{aligned} \begin{bmatrix} g_1 & g_2 \\ g_3 & g_4 \end{bmatrix} k^{-1} &= \begin{bmatrix} \frac{g_1 g_4 - g_2 g_3}{k_1 g_4 - k_2 g_3} & * \\ 0 & \frac{k_1 g_4 - k_2 g_3}{\alpha(k_1 g_4 - k_2 g_3)} \end{bmatrix} \\ &= \begin{bmatrix} \frac{g_1 g_4 - g_2 g_3}{k_1 g_4 - k_2 g_3} & * \\ 0 & \alpha^{-1} \end{bmatrix}. \end{aligned}$$

Note that since $k \in GL(2,\mathbb{Z}_p)$ and $g \in GL(2,\mathbb{Q}_p)$, we have $g_1 g_4 - g_2 g_3 \in \mathbb{Q}_p^{\times}$, $\alpha(k_1 g_4 - k_2 g_3) \in \mathbb{Z}_p^{\times}$, hence $\alpha \neq 0$, $k_1 g_4 - k_2 g_3 \neq 0$. □

Now, we will state and prove Iwasawa's theorem.

Theorem 3.4.3. *Let $g \in GL(2,\mathbb{Q}_p)$, then $\exists\, a, d \in \mathbb{Q}_p^{\times}, b \in \mathbb{Q}_p$ and $k \in GL(2,\mathbb{Z}_p)$ such that*

$$g = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} k,$$

where this factorization is unique in the following sense if

$$g = \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix} k_1 = \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} k_2,$$

where $a_1, a_2, d_1, d_2 \in \mathbb{Q}_p^\times, b_1, b_2 \in \mathbb{Q}_p$ *and* $k_1, k_2 \in GL(2, \mathbb{Z}_p)$*, then*

$$|a_1|_p = |a_2|_p \text{ and } |d_1|_p = |d_2|_p.$$

Proof. Suppose that $g = \begin{bmatrix} g_1 & g_2 \\ g_3 & g_4 \end{bmatrix} \in GL(2, \mathbb{Q}_p)$, hence

$$|g_3|_p = p^n \quad and \quad |g_4|_p = p^m,$$

where $n, m \in \mathbb{Z}$. Assume without loss of generality that $n \geq m$, then

$$\begin{aligned} |p^n g_3|_p &= p^{-n} p^n \\ &= 1 \Rightarrow p^n g_3 \in \mathbb{Z}_p^\times \subseteq \mathbb{Z}_p. \end{aligned}$$

$$\begin{aligned} |p^n g_4|_p &= p^{-n} p^m \\ &= \frac{1}{p^{n-m}} \Rightarrow p^n g_4 \in \mathbb{Z}_p. \end{aligned}$$

By lemma 3.4.1, as we have $p^n g_3 \in \mathbb{Z}_p^\times$ and $p^n g_4 \in \mathbb{Z}_p$, then $\exists\, r, s \in \mathbb{Z}_p$ such that

$$\begin{bmatrix} r & s \\ p^n g_3 & p^n g_4 \end{bmatrix} \in GL(2, \mathbb{Z}_p).$$

Take

$$k := \begin{bmatrix} r & s \\ p^n g_3 & p^n g_4 \end{bmatrix} \in GL(2, \mathbb{Z}_p).$$

We have that the bottom row of k is a p^n multiple of the bottom row of g which by the previous lemma implies that

$$g = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} k,$$

where $a, d \in \mathbb{Q}_p^\times$ and $b \in \mathbb{Q}_p$.

Now for the uniqueness part, assume that

$$g = \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix} k_1 = \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} k_2,$$

where $a_1, a_2, d_1, d_2 \in \mathbb{Q}_p^\times, b_1, b_2 \in \mathbb{Q}_p$ *and* $k_1, k_2 \in GL(2, \mathbb{Z}_p)$. We should prove that

$$|a_1|_p = |a_2|_p \text{ and } |d_1|_p = |d_2|_p.$$

We have

$$g = \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix} k_1 = \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} k_2.$$

This implies that

$$\begin{aligned} k_1 k_2^{-1} &= \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix}^{-1} \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} \\ &= \begin{bmatrix} \frac{d_1}{a_1 d_1} & \frac{-b_1}{a_1 d_1} \\ 0 & \frac{a_1}{a_1 d_1} \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} \\ &= \begin{bmatrix} a_1^{-1} a_2 & * \\ 0 & d_1^{-1} d_2 \end{bmatrix} \in GL(2, \mathbb{Z}_p). \end{aligned}$$

Therefore, $a_1^{-1} a_2$, $d_1^{-1} d_2 \in \mathbb{Z}_p$, and $a_1^{-1} a_2 d_1^{-1} d_2 \in \mathbb{Z}_p^\times$

$\implies |a_1^{-1} a_2|_p \leq 1$, $|d_1^{-1} d_2|_p \leq 1$, and $|a_1^{-1} a_2 d_1^{-1} d_2|_p = 1$

$\implies |a_1^{-1} a_2|_p = |d_1 d_2^{-1}|_p$.

But since $|d_1^{-1} d_2|_p \leq 1$, it follows that $|d_1 d_2^{-1}|_p \geq 1$

$\implies 1 \geq |a_1^{-1} a_2|_p = |d_1 d_2^{-1}|_p \geq 1$

$\implies |a_1^{-1} a_2|_p = |d_1 d_2^{-1}|_p = 1$

$\implies |a_1|_p = |a_2|_p$ and $|d_1|_p = |d_2|_p$. □

3.5 THE SPACE $V(\chi_1, \chi_2)$

Given two quasi characters χ_1, χ_2, the space $V(\chi_1, \chi_2)$ is defined to be the space of all locally functions $f : GL(2, \mathbb{Q}_p) \to \mathbb{C}$ satisfying some certain condition. In this section, we will introduce the space $V(\chi_1, \chi_2)$ and see how its elements look like.

Definition. Fix $s_1, s_2 \in \mathbb{C}$, then the space of functions $V_p(s_1, s_2)$ is defined to be all the functions $f : GL(2, \mathbb{Q}_p) \longrightarrow \mathbb{C}$ that satisfy

$$f\left(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} k\right) = |a|_p^{s_1}|d|_p^{s_2} f(k)$$

where $a, d \in \mathbb{Q}_p^{\times}$, $b \in \mathbb{Q}_p$, $k \in GL(2, \mathbb{Q}_p)$.

Lemma 3.5.1. *The space $V_p(s_1, s_2)$ is not empty.*

Proof. We claim that f^0 defined by

$$f^0\left(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} k\right) = |a|_p^{s_1}|d|_p^{s_2},$$

where $a, d \in \mathbb{Q}_p^{\times}$, $b \in \mathbb{Q}_p$, $k \in GL(2, \mathbb{Z}_p)$, is a well defined function in $V_p(s_1, s_2)$.

Assume

$$g = \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix} k_1 = \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} k_2,$$

where $a_1, d_1, a_2, d_2 \in \mathbb{Q}_p^{\times}, b_1, b_2 \in \mathbb{Q}_p$, $k_1, k_2 \in GL(2, \mathbb{Z}_p)$. Then, by Iwasawa's theorem, we have

$$|a_1|_p = |a_2|_p \quad \text{and} \quad |d_1|_p = |d_2|_p.$$

Hence,

$$|a_1|_p^{s_1}|d_1|_p^{s_2} = |a_2|_p^{s_1}|d_2|_p^{s_2},$$

therefore

$$f^0\left(\begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix} k_1\right) = f^0\left(\begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} k_2\right).$$

□

Let χ_1 χ_2 be two quasi characters. Now, we want to generalize the space of functions $V(s_1, s_2)$.

Definition. The space of function $V(\chi_1, \chi_2)$ is defined to be all the locally constant functions $f : GL(2, \mathbb{Q}_p) \to \mathbb{C}$ satisfying

$$f\left(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} k\right) = \chi_1(a)\chi_2(d)f(k), \text{ where } a, d \in \mathbb{Q}_p^\times, b \in \mathbb{Q}_p, k \in GL(2, \mathbb{Q}_p).$$

Remark. One could try to generalize f^0 above, however, f^0 here is not well defined.

$$f^0\left(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} k\right) = \chi_1(a)\chi_2(d),$$

where $a, d \in \mathbb{Q}_p^\times$, $b \in \mathbb{Q}_p$, $k \in GL(2, \mathbb{Q}_p)$

f^0 is not well defined. Note that f^0 will be well defined if

$$\chi_1(a_1) = \chi_1(a_2),$$

and

$$\chi_2(a_1) = \chi_2(a_2),$$

whenever $|a_1|_p = |a_2|_p$. In other words, f^0 will be well defined if χ_1, χ_2 send all elements that have the same absolute value to the same element in $\mathbb{C}$.

Lemma 3.5.2. *Let $f \in V(\chi_1, \chi_2)$, then $\exists\, m \in \mathbb{N}$ such that $f|_{gK(p^m)}$ is constant $\forall g \in GL(2, \mathbb{Q}_p)$.*

Proof. Let $f \in V(\chi_1, \chi_2)$. Then $f : GL(2, \mathbb{Q}_p) \to \mathbb{C}$ is locally constant and

$$f\left(\left[\begin{array}{cc} a & b \\ 0 & d \end{array}\right] k\right) = \chi_1(a)\chi_2(d)f(k),$$

where $a, d \in \mathbb{Q}_p^{\times}$, $b \in \mathbb{Q}_p$, $k \in GL(2, \mathbb{Q}_p)$. Now, since f is locally constant, then by lemma 3.3.4, there exists an $m \in \mathbb{N}$ such that $f|_{gK(p^m)}$ is constant $\forall g \in GL(2, \mathbb{Z}_p)$. Now, from Iwasawa's theorem, we have that for all $g \in GL(2, \mathbb{Q}_p)$ g can be decomposed as $g = \left[\begin{array}{cc} a & b \\ 0 & d \end{array}\right] k$, where $a, d \in \mathbb{Q}_p^{\times}$, $b \in \mathbb{Q}_p$ and $k \in GL(2, \mathbb{Z}_p)$. Now, let $k' \in K(p^m)$ then $f(gk') = f(\left[\begin{array}{cc} a & b \\ 0 & d \end{array}\right] kk') = \chi_1(a)\chi_2(d)f(kk') = \chi_1(a)\chi_2(d)f(k) = f(\left[\begin{array}{cc} a & b \\ 0 & d \end{array}\right] k) = f(g)$. Hence, we conclude that

$$f|_{gK(p^m)} \text{is constant } \forall g \in GL(2, \mathbb{Q}_p).$$

□

Lemma 3.5.3. *Let $f \in V(\chi_1, \chi_2)$, then f is completely determined by its restriction on $GL(2, \mathbb{Z}_p)$.*

Proof. Let $f_1, f_2 \in V(\chi_1, \chi_2)$ such that

$$f_1|_{GL(2,\mathbb{Z}_p)} = f_2|_{GL(2,\mathbb{Z}_p)}.$$

We have to show that

$$f_1(g) = f_2(g),$$

$\forall g \in GL(2, \mathbb{Q}_p)$. Let $g \in GL(2, \mathbb{Q}_p)$, then by Iwasawa's theorem, we have $g = \left[\begin{array}{cc} a & b \\ 0 & d \end{array}\right] k$, where $a, d \in \mathbb{Q}_p^{\times}$, $d \in \mathbb{Q}_p$ and $k \in GL(2, \mathbb{Z}_p)$. Now, $f_1(g) = f_1\left(\left[\begin{array}{cc} a & b \\ 0 & d \end{array}\right] k\right) =$

$$\chi_1(a)\chi_2(d)f_1(k) = \chi_1(a)\chi_2(d)f_2(k) = f_2\left(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} k\right) = f_2(g). \qquad \square$$

Lemma 3.5.4. *Let χ_1, χ_2 be quasi characters and let $n = max(cond(\chi_1), cond(\chi_2))$. Then, the formula f defined by*

$$f\left(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} k\right) = \begin{cases} \chi_1(a)\chi_2(d) & : k \in K(p^n) \\ 0 & : k \notin K(p^n) \end{cases}$$

gives a well-defined element of $V(\chi_1, \chi_2)$.

Proof. We should show that f is well defined. Assume

$$g = \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix} k_1 = \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} k_2,$$

which implies that

$$\begin{aligned} k_1 k_2^{-1} &= \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix}^{-1} \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} \\ &= \begin{bmatrix} \frac{d_1}{a_1 d_1} & \frac{-b_1}{a_1 d_1} \\ 0 & \frac{a_1}{a_1 d_1} \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} \\ &= \begin{bmatrix} a_1^{-1}a_2 & * \\ 0 & d_1^{-1}d_2 \end{bmatrix} \in K(p^n). \end{aligned}$$

Hence, $a_1 a_2^{-1} \equiv 1 \bmod(p^n)$ and $d_1 d_2^{-1} \equiv 1 \bmod(p^n)$. This implies that $a_1 a_2^{-1} = 1 + k_1 p^n$ and $d_1 d_2^{-1} = 1 + k_2 p^n$, where $k_1, k_2 \in \mathbb{Z}_p$. Therefore, $\chi_1(a_1 a_2^{-1}) = \chi_1(1 + k_1 p^n) = 1$ and so $\chi_1(a_1 a_2^{-1}) = 1$ and as χ_1 is a homomorphism we have $1 = \chi_1(a_1 a_2^{-1}) = \chi_1(a_1)\chi_1(a_2)^{-1} = \frac{\chi_1(a_1)}{\chi_1(a_2)}$, we conclude that $\chi_1(a_1) = \chi_1(a_2)$. Similarly, we get $\chi_2(d_1) = \chi_2(d_2)$, which completes the proof. $\square$

Now, let the group $GL(2,\mathbb{Q}_p)$ act on the space $V(\chi_1,\chi_2)$, by:

$$[\rho(g).f](x) = f(xg).$$

Lets now check that it is an action:

(1) $[\rho(I).f](g) = f(gI) = f(g)$,

(2) $[\rho(k_1)[\rho(k_2).f]](g) = [\rho(k_2)f](gk_1) = f(gk_1k_2)) = [\rho(k_1k_2).f](g)$.

Remark.

Let $m \in \mathbb{N}$. The space $V(\chi_1,\chi_2)^{K(p^m)} = \{f \in V(\chi_1,\chi_2)$ such that $[\rho(k).f](g) = f(gk) = f(g),\ \forall g \in GL(2,\mathbb{Q}_p)\} = \{f \in V(\chi_1,\chi_2)$ such that $\rho(k).f = f\}$. Since we have $K(p) \supset K(p^2) \supset K(p^3) \supset \ldots$, then it follows that

$$V(\chi_1,\chi_2)^{K(p)} \subset V(\chi_1,\chi_2)^{K(p^2)} \subset \ldots .$$

Theorem 3.5.5. *We have* $V(\chi_1,\chi_2) = \bigcup_{m=1}^{\infty} V(\chi_1,\chi_2)^{K(p^m)}$.

Proof. Let $f \in \bigcup_{m=1}^{\infty} V(\chi_1,\chi_2)^{K(p^m)}$, then $f \in V(\chi_1,\chi_2)^{K(p^n)}$ for some $n \in \mathbb{N}$, and hence $f \in V(\chi_1,\chi_2)$ and so

$$V(\chi_1,\chi_2) \supseteq \bigcup_{m=1}^{\infty} V(\chi_1,\chi_2)^{K(p^m)}.$$

Let $f \in V(\chi_1,\chi_2)$, then by lemma 3.5.2 $\exists\, n \in \mathbb{N}$ such that $f(kg) = f(g)\ \forall g \in GL(2,\mathbb{Q}_p), \forall k \in K(p^n)$. Therefore, $f \in V(\chi_1,\chi_2)^{K(p^n)}$ which implies $f \in \bigcup_{m=1}^{\infty} V(\chi_1,\chi_2)^{K(p^m)}$. This implies that

$$V(\chi_1,\chi_2) \subseteq \bigcup_{m=1}^{\infty} V(\chi_1,\chi_2)^{K(p^m)},$$

and hence

$$V(\chi_1,\chi_2) = \bigcup_{m=1}^{\infty} V(\chi_1,\chi_2)^{K(p^m)}.$$

□

Let $\zeta \in GL(2,\mathbb{Z}_p)$, and let $n = \max(cond(\chi_1), cond(\chi_2))$. For all $g \in GL(2,\mathbb{Q}_p)$, by Iwasawa's theorem g can be decomposed as $g = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} k$, where $a, d \in \mathbb{Q}_p^{\times}, c \in \mathbb{Q}_p, k \in GL(2,\mathbb{Z}_p)$. Then, define the mapping $f_\zeta : GL(2,\mathbb{Q}_p) \to \mathbb{C}$ by

$$f_\zeta(g) = \begin{cases} \chi_1(a)\chi_2(d) & g \in B(\mathbb{Q}_p)\zeta K(p^n) \\ 0 & g \notin B(\mathbb{Q}_p)\zeta K(p^n) \end{cases}.$$

Lemma 3.5.6. *The function f_ζ defined as above is an element of $V(\chi_1,\chi_2)$.*

Proof. Let

$$g = \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix} \zeta k_1 = \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} \zeta k_2,$$

then

$$\begin{bmatrix} a_2^{-1} & * \\ 0 & d_2^{-1} \end{bmatrix} \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix} = \zeta k_2 k_1^{-1} \zeta^{-1}.$$

The element $k_2 k_1^{-1} \in K(p^n)$ since $K(p^n)$ is subgroup, and the element $\zeta(k_2 k_1^{-1})\zeta^{-1}$ is an element of $K(p^n)$ as well (since $K(p^n)$ is normal subgroup in $GL(2,\mathbb{Z}_p)$ by lemma 3.3.2). Hence, we have

$$a_1 a_2^{-1}, d_1 d_2^{-1} \equiv 1 \bmod (p^n),$$

thus

$$a_1 a_2^{-1}, d_1 d_2^{-1} \in 1 + p^n \mathbb{Z}_p.$$

Therefore, $\chi_1(a_1 a_2^{-1}) = 1$, and so $\chi_1(a_1) = \chi_1(a_2)$ and $\chi_2(d_1 d_2^{-1}) = 1$, and so $\chi_2(d_1) = \chi_2(d_2)$, we conclude that f is well defined and therefore f_ζ is an element of $V(\chi_1,\chi_2)$. □

Remark. Consider the set of all double cosets $B(\mathbb{Q}_p)\backslash GL(2,\mathbb{Q}_p)/K(p^m) = \{B(\mathbb{Q}_p)\zeta K(p^m)$ such that $\zeta \in GL(2,\mathbb{Q}_p)\}$. Note that since we have

$$B(\mathbb{Q}_p)\zeta K(p^n) = B(\mathbb{Q}_p)\xi K(p^n) \ \ or \ \ B(\mathbb{Q}_p)\zeta K(p^n) \bigcap B(\mathbb{Q}_p)\xi K(p^n) = \emptyset,$$

then it is enough to choose one representative ζ for each double coset. Furthermore, we can choose this representative to be from $GL(2,\mathbb{Z}_p)$ because for each $g \in GL(2,\mathbb{Q}_p)$, by Iwasawa's theorem, g can be written as $g = qr$, where $q \in B(\mathbb{Q}_p)$, $r \in GL(2,\mathbb{Z}_p)$. Then, the double coset $B(\mathbb{Q}_p)gK(p^n) = B(\mathbb{Q}_p)rK(p^n)$. Hence, let $\Im$ denote a set of representatives for the set of double cosets $B(\mathbb{Q}_p)\backslash GL(2,\mathbb{Q}_p)/K(p^m)$, where the elements of $\Im$ are chosen to be from $GL(2,\mathbb{Z}_p)$.

Lemma 3.5.7. *Let $\Im$ be defined as in the previous remark and let $n = max\left(cond\left(\chi_1\right), cond\left(\chi_2\right)\right)$, then*

$$dim(V\left(\chi_1,\chi_2\right)^{K(p^m)}) = \begin{cases} |\Im| & : m \geq n \\ 0 & : m < n \end{cases},$$

where $|\Im|$ denotes the number of elements in the set $\Im$.

Proof. Let $m \geq n$ and let $\Im$ be defined as in the previous remark, we will prove that the set $\{f_\zeta$ such that $\zeta \in \Im\}$ is a basis for $V\left(\chi_1,\chi_2\right)^{K(p^m)}$ and then we are done.

Let $f \in V\left(\chi_1,\chi_2\right)^{K(p^m)}$. Define

$$h := \sum_{\zeta \in \Im} f(\zeta) f_\zeta.$$

Let $g \in GL(2,\mathbb{Q}_p)$, then as $GL(2,\mathbb{Q}_p) = \bigcup_{\zeta\in\Im} B(\mathbb{Q}_p)\zeta K(p^m)$ we have $g \in B(\mathbb{Q}_p)\zeta K(p^m)$ for some $\zeta \in \Im$. Therefore $g = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \zeta k$ where $a, d \in \mathbb{Q}_p^\times, b \in \mathbb{Q}_p$ and $k \in K(p^m)$. Hence, $f(g) = \chi_1(a)\chi_2(d)f(\zeta k) = \chi_1(a)\chi_2(d)f(\zeta)$. On the other hand, we have $h(g) = \sum_{\xi\in\Im} f(\xi) f_\xi(g)$. But by definition of f_ξ

$$f_\xi(g) = \begin{cases} \chi_1(a)\chi_2(d) & : \xi = \zeta \\ 0 & : \xi \neq \zeta \end{cases}.$$

Now, all the terms in this sum are zeros, except for the term $f(\zeta)f_\zeta(g) = f(\zeta)\chi_1(a)\chi_2(d)$. Hence, $h(g) = f(\zeta)\chi_1(a)\chi_2(d) = f(g)$, and as g is arbitrarily chosen from $GL(2,\mathbb{Q}_p)$, we have $f = h$. Now, since f is arbitrarily chosen from $V(\chi_1,\chi_2)^{K(p^m)}$, that is also true for any $f \in V(\chi_1,\chi_2)^{K(p^m)}$, we conclude that the set $\{f_\zeta$ such that $\zeta \in \Im\}$ is a spanning set for $V(\chi_1,\chi_2)^{K(p^m)}$. Now, we should prove that the set $\{f_\zeta$ such that $\zeta \in \Im\}$ is linearly independent. Let

$$\sum_{\zeta\in\Im} c_\zeta f_\zeta = 0.$$

We should show that $c_\zeta = 0\ \forall\zeta \in \Im$. Now, let ξ be given and let's substitute this value into the sum $\sum_{\zeta\in\Im} c_\zeta f_\zeta = 0$. Then $f_\zeta(\xi) = 0$ if $\zeta \neq \xi$. It follows that $c_\xi f_\xi(\xi) = 0$. But we have $f_\xi(\xi) = f_\xi(I\xi I) = 1$, we conclude that $c_\xi = 0$ and as ξ is arbitrarily chosen from the set $\Im$, then we have $c_\xi = 0$ for each $\xi \in \Im$.

Now, to prove the case where $m < n$, I want to prove first that given $m \in \mathbb{N}$ and $f \in V(\chi_1,\chi_2)^{K(p^m)}$, then $f(kx) = f(x)$ for all $k \in K(p^m)$, $x \in GL(2,\mathbb{Z}_p)$. Let $f \in V(\chi_1,\chi_2)^{K(p^m)}$, then $f(xk) = f(x)$ for all $k \in K(p^m)$, $x \in GL(2,\mathbb{Q}_p)$. Now, let $x \in GL(2,\mathbb{Z}_p)$, $k \in K(p^m)$, then $f(kx) = f(xx^{-1}kx) = f(x(x^{-1}kx)) = f(x)$ (since by lemma 3.3.2 $K(p^m)$ is normal in $GL(2,\mathbb{Z}_p)$ and hence $x^{-1}kx \in K(p^m)$). Now, suppose that $m < n$, we want to show that $V(\chi_1,\chi_2)^{K(p^m)} = 0$. I will split the proof into two cases:

Case(a): If $\max(n_1,n_2)=n_1$ then $m < n_1$, and hence there is some $a \in 1+p^m\mathbb{Z}_p$ such that $\chi_1(a) \neq 1$ and therefore note that $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in K(p^m)$. Therefore, given $f \in V(\chi_1,\chi_2)^{K(p^m)}$ $\chi_1(a)\chi_2(1)f(g) = f(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} g) = f(g)$ for all $g \in GL(2,\mathbb{Z}_p)$, thus $\chi_1(a)f(g) = f(g)$ for all $g \in GL(2,\mathbb{Z}_p)$ and $\chi_1(a) \neq 1$, hence $f(g) = 0$ for all $g \in GL(2,\mathbb{Z}_p)$, then for any $g' \in GL(2,\mathbb{Q}_p)$ by Iwasawa's theorem, we can decompose g' as $g' = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} g$ where

$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in B(\mathbb{Q}_p)$, $g \in GL(2,\mathbb{Z}_p)$, and then $f(g') = f(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} g) = \chi_1(a)\chi_2(d)f(g) = \chi_1(a)\chi_2(d).0 = 0$. We conclude that $f(g) = 0$ for all $g \in GL(2,\mathbb{Q}_p)$, and as f is chosen arbitrarily from $V(\chi_1,\chi_2)^{K(p^m)}$, then $V(\chi_1,\chi_2)^{K(p^m)} = 0$.

Case(b): If $\max(n_1,n_2)$ is n_2 then $m < n_2$. Hence, there is some $a \in 1 + p^m\mathbb{Z}_p$ such that $\chi_2(a) \neq 1$ and as a result note that $\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \in K(p^m)$, and so given $f \in V(\chi_1,\chi_2)^{K(p^m)}$ $\chi_1(1)\chi_2(a)f(g) = f(\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} g) = f(g)$ for all $g \in GL(2,\mathbb{Z}_p)$. Therefore, $\chi_2(a)f(g) = f(g)$ for all $g \in GL(2,\mathbb{Z}_p)$, where $\chi_2(a) \neq 1$. So, $f(g) = 0$ for all $g \in GL(2,\mathbb{Z}_p)$ and then for any $g' \in GL(2,\mathbb{Q}_p)$ by Iwasawa's theorem, we can decompose g' as $g' = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} g$ where $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in B(\mathbb{Q}_p)$, $g \in GL(2,\mathbb{Z}_p)$. Then, $f(g') = f(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} g) = \chi_1(a)\chi_2(d)f(g) = \chi_1(a)\chi_2(d).0 = 0$. We conclude that $f(g) = 0$ for all $g \in GL(2,\mathbb{Q}_p)$ and as f is chosen arbitrarily from $V(\chi_1,\chi_2)^{K(p^m)}$, we have $V(\chi_1,\chi_2)^{K(p^m)} = 0$. □

CHAPTER 4

NEWFORMS OF $V(\chi_1, \chi_2)$

Our main concern in this chapter is to find the newforms $V(\chi_1, \chi_2)$. Indeed, casselman tells us how to do that. We will follow his proof to find the newforms of $V(\chi_1, \chi_2)$. The material in this chapter is taken from [1] and [5].

Definition. If V is a vector space over the field $\mathbb{F}$, the general linear group of V, written $GL(V)$ or $Aut(V)$, is the group of all automorphisms of V, i.e., the set of all bijective linear transformations V to V, together with functional composition as group operation. If V has finite dimension n, then $GL(V)$ and $GL(n, \mathbb{F})$ are isomorphic.

Definition. A representation of a group G on a vector space V over a field K is a group homomorphism ρ from G to $GL(V)$. That is, a representation is a map:

$$\rho : G \to GL(V),$$

such that

$$\rho(g_1 g_2) = \rho(g_1)\rho(g_2).$$

Here, V is called the representation space, and dimension of V is called the dimension of the representation.

Remark. It is common to refer to V itself as the representation if the homomorphism ρ is clear from the context.

Definition. Let (ρ, V) be a representation of G. A subspace $W \subseteq V$ is said to be stable or G-invariant if $\rho(g)(w) \in W$ $\forall g \in G$, $\forall w \in W$.

Remark. If we have $W \subset V$ which is stable, then $(\rho|_w, W)$ is a representation of G, or, a sub-representation.

Definition. A representation $V \neq 0$ of G is said to be irreducible if the only sub-representations of it are 0 and V. In other words, if V and 0 are the only stable subspaces of V.

Definition. The topological field is defined to be a field where the addition, the product and the inverse functions are continuous.

Definition. Let X be a topological space and let U be an open set, then the closure of the set U denoted by $U^{'}$, is defined to be the intersection of all closed sets containing U.

Definition. A locally compact field $\mathbb{F}$ is a topological field where every element $x \in \mathbb{F}$ has a neighborhood U whose closure $U^{'}$ is compact.

Definition. A local field is a locally compact topological field with respect to a non-discrete topology.

Theorem 4.0.8. *Suppose that $\mathbb{F}$ is a local field, then, we can construct an absolute value on it such that this absolute value induces the topology on $\mathbb{F}$.*

Definition. There are two basic types of local field, those in which the absolute value is archimedean and those in which it is not. In the first case, one calls the local field an archimedean local field, in the second case, one calls it a non-archimedean local field.

Definition. Let k be a non-archimedean local field. Then a (complex) admissible representation of $GL_n(k)$ is a complex vector space V equipped with an action of $GL(n, K)$ (which of course means a group homomorphism $\rho : GL(n, k) \to GL(V)$) such that:
(1) If $U \subset GL(n, k)$ is an open subgroup then

$$V^U = \{v \in V \text{ such that } \rho(u)(v) = v, \forall u \in U\},$$

is finite dimensional,
(2) If $v \in V$ then

$$stab(v) = \{u \in GL(n,k) \text{ such that } \rho(u)(v) = v\},$$

is open subgroup in $GL(n,k)$.

Remark. In the previous definition, there are two relevant fields, the field K where the matrices are taken over, and the field $\mathbb{C}$ where the representation space V is over.

Definition. Let k be a local field with an absolute value $|\ |$. Then, we define the ring of integers by

$$O_k = \{x \in k \text{ such that } |x| \leq 1\}.$$

Definition. Let k be locally compact non-archimedean field, a quasi character of $k^\times$ is defined to be a continuous homomorphism $\epsilon : k^\times \to \mathbb{C}$.

Definition. Let k be a locally compact non-archimedean field and let O_k be its ring of integers and for any ideal $\mathfrak{b}$ define the the subgroup:

$$\Gamma_0(\mathfrak{b}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(O_k) | c \equiv 0 \pmod{\mathfrak{b}} \right\}.$$

Definition. A scalar matrix, is a diagonal matrix in which all the diagonal elements are equal.

Now, we will state Casselman's theorem.

Theorem 4.0.9. *Let k be a non-archimedean local field and let ρ be irreducible admissible infinite dimensional representation of $GL(2,k)$ and let W be the representation space. Define ϵ to be the quasi character of $k^\times$ such that $\rho = \epsilon$ on the scalar matrices. Let $\mathfrak{c}(\rho)$ be the largest ideal of O_k such that the space of vectors:*

$$V(\rho, \mathfrak{c}(\rho)) = \left\{ \rho(\begin{pmatrix} a & b \\ c & d \end{pmatrix})(v) = \epsilon(a)v \ \forall \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\mathfrak{c}(\rho)) \right\},$$

is not trivial. Then this space has dimension one.

Definition. The ideal $\mathfrak{c}(\rho)$ in the previous theorem is called the conductor of ρ.

Definition. The elements of the space $V(\rho, \mathfrak{c}(\rho))$, are called newforms.

In this paper, we are interested in the special case where we have, $k = \mathbb{Q}_p$, $O_k = \mathbb{Z}_p$, and the representation space is $W = V(\chi_1, \chi_2)$, with the representation map ρ is

$$\rho : GL_2(\mathbb{Q}_p) \to GL(V(\chi_1, \chi_2))$$

by

$$\rho(g)(f(x)) = f(xg).$$

Note that from lemma 2.2.7, as $\mathfrak{c}(\rho)$ is an ideal in $\mathbb{Z}_p$, then we have we $\mathfrak{c}(\rho) = p^k\mathbb{Z}_p$ for some $k \in \mathbb{Z}$.

Remark. Now, since we have the inclusion $\mathbb{Z}_p \supset p\mathbb{Z}_p \supset p^2\mathbb{Z}_p \supset ...$ then saying that the conductor $\mathfrak{c}(\rho) = p^k\mathbb{Z}_p$ is the largest ideal such that $V(\rho, p^k\mathbb{Z}_p) \neq 0$ is equivalent to saying that k is the smallest integer where the space $V(\rho, p^k\mathbb{Z}_p) \neq 0$, and so from now and on, I will be denoting the space $V(\rho, \mathfrak{c}(\rho)) = V(\rho, p^k\mathbb{Z}_p)$ simply by $V(\rho, k)$. In general, given $k \in \mathbb{N}$, I will denote $\Gamma_0(p^k\mathbb{Z}_p)$ simply by $\Gamma_0(k)$.

Remark. Let V be a vector space over $\mathbb{C}$. Then, a non-zero element $z \in \mathbb{C}$ can be thought of as a 1-1 onto function from V to V (we consider the mapping $z : V \to V$ by $z(v) = zv$ which is just a scalar multiplication by z).

Lemma 4.0.10. *In the special case where $k = \mathbb{Q}_p$, $O_k = \mathbb{Z}_p$, the representation space $W = V(\chi_1, \chi_2)$, and the representation map is $\rho : GL(2, \mathbb{Q}_p) \to GL(V(\chi_1, \chi_2))$ by $\rho(g)(f(x)) = f(xg)$, we have the space $V(\rho, k)$ is the set of all elements of the form*

$$V(\rho, k) =$$

$$\left\{ f \in V(\chi_1, \chi_2) \mid f(x \begin{pmatrix} a & b \\ c & d \end{pmatrix}) = \chi_1\chi_2(a)f(x) \text{ where } x \in GL(2, \mathbb{Q}_p), \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(k) \right\}.$$

Proof. Since the vector space W in this case is $V(\chi_1, \chi_2)$, and the representation map is $\rho : GL(2, \mathbb{Q}_p) \to GL(V(\chi_1, \chi_2))$ by $\rho(g)(f(x)) = f(xg)$, then the space we are seeking to determine is actually

$$V(\rho, k) =$$
$$\left\{ f \in V(\chi_1, \chi_2) \mid f(x \begin{pmatrix} a & b \\ c & d \end{pmatrix}) = \epsilon(a) f(x) \text{ where } x \in GL(2, \mathbb{Q}_p), \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(k) \right\}.$$

We have that $\epsilon = \rho$ on the scaler matrix, which implies that $\forall a \in \mathbb{Q}_p^\times$ the following functions are equal, i.e., we have

$$\rho(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}) = \epsilon(a),$$

(where $\epsilon(a)$ is considered as function from $V(\chi_1, \chi_2)$ to $V(\chi_1, \chi_2)$, like I have mentioned in the previous remark). As these two functions are equal, they should be equal on each single element $f \in V(\chi_1, \chi_2)$. Hence

$$\rho \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} (f(x)) = \epsilon(a) f(x),$$

but $\rho \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} (f(x)) = f(x \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}) = f(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} x) = \chi_1(a)\chi_2(a) f(x)$. Therefore,

$$\epsilon(a) f(x) = \chi_1(a)\chi_2(a) f(x),$$

where this equation is true for all $f \in V(\chi_1, \chi_2)$. By what we have done in the previous chapter, we know that the space $V(\chi_1, \chi_2) \neq 0$. We can pick a nonzero $f \in V(\chi_1, \chi_2)$, and then pick an element x, where $f(x) \neq 0$. Then, we can cancel $f(x)$ from the two sides to have

$$\epsilon(a) = \chi_1(a)\chi_2(a).$$

We conclude that

$$V(\rho,k)=$$

$$\left\{ f\in V(\chi_1,\chi_2)\ |f(x\begin{pmatrix} a & b \\ & \\ c & d \end{pmatrix})=\chi_1\chi_2(a)f(x)\ where\ x\in GL(2,\mathbb{Q}_p),\ \begin{pmatrix} a & b \\ & \\ c & d \end{pmatrix}\in\Gamma_0(k) \right\}.$$

□

Definition. Let μ_1, μ_2 be two quasi characters, the space $B(\mu_1,\mu_2)$ is defined to be the space of all locally functions $f: GL(2,\mathbb{Q}_p)\to\mathbb{C}$ satisfying

$$f\left(\begin{pmatrix} a & x \\ & \\ 0 & b \end{pmatrix} g\right)=\mu_1(a)\mu_2(b)|\frac{a}{b}|^{1/2}f(g).$$

where $\begin{pmatrix} a & x \\ & \\ 0 & b \end{pmatrix}\in B(\mathbb{Q}_p)$, $g\in GL(2,\mathbb{Q}_p)$.

Definition. Let μ_1, μ_2 be two quasi characters, the space $B(\mu_1,\mu_2)$ is defined to be the space of all locally functions $f: GL(2,\mathbb{Q}_p)\to\mathbb{C}$ satisfying

$$f\left(\begin{pmatrix} a & x \\ & \\ 0 & b \end{pmatrix} g\right)=\mu_1(a)\mu_2(b)|\frac{a}{b}|^{1/2}f(g).$$

where $\begin{pmatrix} a & x \\ & \\ 0 & b \end{pmatrix}\in B(\mathbb{Q}_p)$, $g\in GL(2,\mathbb{Q}_p)$.

Remark. Given the quasi characters χ_1,χ_2. Define $\mu_1(x):=|x|^{-1/2}\chi_1(x)$, $\mu_2(x):=\chi_2(x)|x|^{1/2}$, then it is easy to see that $B(\mu_1,\mu_2)=V(\chi_1,\chi_2)$.

Definition. Let μ_1, μ_2 be two quasi characters, the space $C(\mu_1,\mu_2)$ is defined to be the space of all locally functions $F: GL(2,\mathbb{Z}_p)\to\mathbb{C}$ satisfying

$$F\left(\begin{pmatrix} a & x \\ & \\ 0 & b \end{pmatrix} g\right)=\mu_1(a)\mu_2(b)F(g),$$

where $\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} \in B(\mathbb{Z}_p)$, $g \in GL(2,\mathbb{Z}_p)$.

Lemma 4.0.11. *The restriction map* $Res : B(\mu_1,\mu_2) \to C(\mu_2,\mu_2)$ *defined by*

$$Res(f) = f|_{GL(2,\mathbb{Z}_p)},$$

is a 1-1 linear onto function.

Proof. (1) $Res(f)$ lands at $C(\mu_2,\mu_2)$:
Let $f \in B(\mu_1,\mu_2)$, then $f\left(\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} g\right) = \mu_1(a)\mu_2(b)|\frac{a}{b}|^{1/2} f(g)$, where $\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} \in B(\mathbb{Q}_p)$, $g \in GL(2,\mathbb{Q}_p)$, and then $Res(f) = f|_{GL(2,\mathbb{Z}_p)}$ satisfies $Res(f) = f|_{GL(2,\mathbb{Z}_p)}\left(\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} g\right) = \mu_1(a)\mu_2(b)|\frac{a}{b}|^{1/2} f(g)$, where $\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} \in B(\mathbb{Z}_p)$, $g \in GL(2,\mathbb{Z}_p)$. Now, since $\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} \in B(\mathbb{Z}_p)$, then $a, b \in \mathbb{Z}_p^\times$ and so $|a| = |b| = 1$. Now, since f is locally constant on $GL(2,\mathbb{Q}_p)$, then it is locally constant on $GL(2,\mathbb{Z}_p)$. From here, we can conclude the function $f|_{GL(2,\mathbb{Z}_p)}$ is an element of $C(\mu_1,\mu_2)$.

(2) $Res(f)$ is a linear function:
(a) $Res(\alpha f) = (\alpha f)|_{GL(2,\mathbb{Z}_p)} = \alpha f|_{GL(2,\mathbb{Z}_p)} = \alpha Res(f)$. Here, given a complex valued function f and $\alpha \in \mathbb{C}$, the function αf is defined by $(\alpha f)(x) = \alpha f(x)$ for all x in the domain of f.
(b)$Res(f+g) = (f+g)|_{GL(2,\mathbb{Z}_p)} = f|_{GL(2,\mathbb{Z}_p)} + g|_{GL(2,\mathbb{Z}_p)} = Res(f) + Res(g)$, as for any two complex valued functions having the same domain, the function $f+g$ is defined by $(f+g)(x) = f(x) + g(x)$ for all x in the domain of f and g.
(3) $Res(f)$ is injective:
Assume we have $Res(f) = f|_{GL(2,\mathbb{Z}_p)} = g|_{GL(2,\mathbb{Z}_p)} = Res(g)$, then we have to show that

$f(y) = g(y)\ \forall y \in GL(2,\mathbb{Q}_p)$. Let $y \in GL(2,\mathbb{Q}_p)$, then by Iwasawa's theorem there exists $\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} \in B(\mathbb{Q}_p)$, $k \in GL(2,\mathbb{Z}_p)$ such that $y = \begin{pmatrix} a & x \\ 0 & b \end{pmatrix} k$, and then $f(y) = f(\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} k) = \mu_1(a)\mu_2(b)|\frac{a}{b}|^{1/2} f(k) = \mu_1(a)\mu_2(b)|\frac{a}{b}|^{1/2} g(k) = g(\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} k) = g(y)$.

(4) To show that Res is surjective: Let $F \in C(\mu_1,\mu_1)$. I claim that $Res(F)^{-1} = f \in B(\mu_1,\mu_1)$ such that $f(\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} k) = \mu_1(a)\mu_2(b)|\frac{a}{b}|^{1/2} F(k)$ for all $\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} \in B(\mathbb{Q}_p)$, $k \in GL(2,\mathbb{Z}_p)$. Now, we have to prove two things which are that f is a well-defined element of $B(\mu_1,\mu_2)$ and $Res(f) = F$.

(a) To show that f is a well-defined element of $B(\mu_1,\mu_2)$:

Assume we have

$$g = \begin{pmatrix} a_1 & x_1 \\ 0 & b_1 \end{pmatrix} k_1 = \begin{pmatrix} a_2 & x_2 \\ 0 & b_2 \end{pmatrix} k_2,$$

where $\begin{pmatrix} a_1 & x_1 \\ 0 & b_1 \end{pmatrix}, \begin{pmatrix} a_2 & x_2 \\ 0 & b_2 \end{pmatrix} \in B(\mathbb{Q}_p)$, $k_1, k_2 \in GL(2,\mathbb{Z}_p)$, then we have

$$\begin{pmatrix} a_1 a_2^{-1} & * \\ 0 & b_1 b_2^{-1} \end{pmatrix} k_1 = k_2,$$

and hence $F(k_2) = \mu_1(a_1)\mu_1(a_2^{-1})\mu_2(b_1)\mu_2(b_2^{-1})F(k_1)$, and so $f(\begin{pmatrix} a_2 & x_2 \\ 0 & b_2 \end{pmatrix} k_2) = \mu_1(a_2)\mu_2(b_2)F(k_2) = \mu_1(a_2)\mu_2(b_2)\mu_1(a_1)\mu_1(a_2^{-1})\mu_2(b_1)\mu_2(b_2^{-1})F(k_1) = \mu_1(a_1)\mu_2(b_1)F(k_1) = f(\begin{pmatrix} a_1 & x_1 \\ 0 & b_1 \end{pmatrix} k_1)$, we conclude that f is a well-defined function in $B(\mu_1,\mu_2)$.

(b) Lets now prove that $Res(f) = F$:

We know that $Res(f) = f|_{GL(2,\mathbb{Z}_p)}$, and so we have to show

$$f(k) = F(k),$$

for all $k \in GL(2,\mathbb{Z}_p)$. Let $k \in GL(2,\mathbb{Z}_p)$, then $f(k) = f(Ik) = \mu_1(1)\mu_2(1)F(k) = F(k)$. This completes the proof of lemma 4.0.11 . □

Remark. From now and on, for simplicity, I will denote the restriction function Res by R instead,i.e., $R := Res$ and therefore $R : B(\mu_1, \mu_2) \to C(\mu_1, \mu_2)$ is an isomorphism.

Remark. The space of functions $C(\mu_1, \mu_2)$ is a representation of $GL(2,\mathbb{Z}_p)$, where the representation homomorphism is

$$r : GL(2,\mathbb{Z}_p) \to GL(C(\mu_1, \mu_2)),$$

and hence given $k \in GL(2,\mathbb{Z}_p)$ we have

$$r(k) : C(\mu_1, \mu_2) \to C(\mu_1, \mu_2),$$

by $r(k)(F(y)) = F(yk)$ for each $y \in GL(2,\mathbb{Z}_p)$ is a 1-1 onto linear function.

Definition. Let V, W be vector spaces, let H and G be groups such that $H \subseteq G$, and let $\phi : V \to W$ be an isomorphism. Let

$$\rho : G \to GL(V),$$

$$r : H \to GL(W),$$

be two representations of the groups G, H on V, W respectively. Then, we say that ϕ is an *H- isomorphism* if for each $h \in H$, $v \in V$ we have

$$r(h)(\phi(v)) = \phi(\rho(h)(v)).$$

Lemma 4.0.12. *Considering the vector spaces $B(\mu_1, \mu_2)$, $C(B(\mu_1, \mu_2)$, the groups $GL(2,\mathbb{Z}_p)$, $GL(2,\mathbb{Q}_p)$, the representations ρ and r defined as in this chapter, then the isomorphism R is a $GL(2,\mathbb{Z}_p)$ isomorphism.*

Proof. Let $f \in B(\mu_1, \mu_2)$, $k \in GL(2, \mathbb{Z}_p)$ and let $g := \rho(k)(f)$ which is an element of $B(\mu_1, \mu_2)$ such that $g(x) = f(xk)$. We have to show that $r(k)(R(f)) = R(\rho(k)(f))$. As both sides of the equation are functions, we have to show that they are equal at each single element $x \in GL(2, \mathbb{Z}_p)$. Now, $[r(k)(R(f))](x) = [r(k)(f|_{GL(2,\mathbb{Z}_p)})](x) = f|_{GL(2,\mathbb{Z}_p)}(xk) = f(xk)$ since $x, k \in GL(2, \mathbb{Z}_p)$. On the other hand, $R(\rho(k)(f))(x) = R(g)(x) = g|_{GL(2,\mathbb{Z}_p)}(x) = g(x) = f(xk)$ which completes the proof. □

Corollary 4.0.13. *The space $V(\rho, k)$ is isomorphic to the space $R(V(\rho, k))$, i.e.,*

$$V(\rho, k) \cong R(V(\rho, k)).$$

Proof. The restriction function restricted on $V(\rho, k)$

$$R|_{V(\rho,k)} : V(\rho, k) \to R(V(\rho, k)),$$

is a 1-1 onto linear function. It is 1-1 linear function as R is and it is onto as its range it defined to be $R(V(\rho, k))$. □

Definition. The space $C(\mu_1, \mu_2, k)$ is defined to be the space of all functions $F \in C(\mu_1, \mu_2)$ satisfying

$$F(x \begin{pmatrix} a & b \\ c & d \end{pmatrix}) = \mu_1(a)\mu_2(a)F(x),$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(k), x \in GL(2, \mathbb{Z}_p)$.

Lemma 4.0.14. *Let R denote the restriction function defined as before, then*

$$C(\mu_1, \mu_2, k) = R(V(\rho, k)).$$

Proof. The space $R(V(\rho, k))$ is equal to the space of all elements $F \in C(\mu_1, \mu_2)$ such that $F = R(f)$, where $f \in V(\rho, k)$ or it is all the functions $F \in C(\mu_1, \mu_2)$ such that $F = R(f)$,

where $f \in B(\mu_1, \mu_2)$ and f satisfies

$$f(x \begin{pmatrix} a & b \\ & \\ c & d \end{pmatrix}) = \mu_1(a)\mu_2(a)f(x),$$

for all $\begin{pmatrix} a & b \\ & \\ c & d \end{pmatrix} \in \Gamma_0(k), x \in GL(2, \mathbb{Q}_p)$. Hence, $F = R(f) = f|_{GL(2,\mathbb{Z}_p)}$ satisfies

$$F(x \begin{pmatrix} a & b \\ & \\ c & d \end{pmatrix}) = \mu_1(a)\mu_2(a)F(x),$$

for all $\begin{pmatrix} a & b \\ & \\ c & d \end{pmatrix} \in \Gamma_0(k), x \in GL(2, \mathbb{Z}_p)$. Therefore, the set $R(V(\rho, k))$ is the set of all $F \in C(\mu_1, \mu_2)$ such that

$$F(x \begin{pmatrix} a & b \\ & \\ c & d \end{pmatrix}) = \mu_1(a)\mu_2(a)F(x),$$

for all $\begin{pmatrix} a & b \\ & \\ c & d \end{pmatrix} \in \Gamma_0(k), x \in GL(2, \mathbb{Z}_p)$ which is the space $C(\mu_1, \mu_2, k)$ by definition. □

Lemma 4.0.15. *The space $C(\mu_1, \mu_2, k)$ is equal to the space of all functions $F \in C(\mu_1, \mu_2)$ satisfying*

$$F(\begin{pmatrix} a & x \\ & \\ 0 & b \end{pmatrix} g \begin{pmatrix} a' & b' \\ & \\ c' & d' \end{pmatrix}) = \mu_1(a)\mu_2(b)\mu_1\mu_2(a')F(g),$$

$\forall\, g \in GL(2, \mathbb{Z}_p)$, *and* $\begin{pmatrix} a & x \\ & \\ 0 & b \end{pmatrix} \in B(\mathbb{Z}_p), \begin{pmatrix} a' & b' \\ & \\ c' & d' \end{pmatrix} \in \Gamma_0(k)$.

Proof. Let $F \in C(\mu_1, \mu_2, k)$. Then $F \in C(\mu_1, \mu_2)$ and $F(g \begin{pmatrix} a^{'} & b^{'} \\ c^{'} & d^{'} \end{pmatrix}) = \mu_1\mu_2(a^{'})F(g)$ $\forall\, g \in GL(2, \mathbb{Z}_p), \begin{pmatrix} a^{'} & b^{'} \\ c^{'} & d^{'} \end{pmatrix} \in \Gamma_0(k)$. Now, since $F \in C(\mu_1, \mu_2)$ we have $F(\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} g^{'}) = \mu_1(a)\mu_2(b)F(g^{'})$ for all $\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} \in B(\mathbb{Z}_p), g^{'} \in GL(2, \mathbb{Z}_p)$. Choose $g^{'} = g \begin{pmatrix} a^{'} & b^{'} \\ c^{'} & d^{'} \end{pmatrix}$, then we have $F(\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} g \begin{pmatrix} a^{'} & b^{'} \\ c^{'} & d^{'} \end{pmatrix}) = \mu_1(a)\mu_2(b)F(g \begin{pmatrix} a^{'} & b^{'} \\ c^{'} & d^{'} \end{pmatrix}) = \mu_1(a)\mu_2(b)\mu_1\mu_2(a^{'})F(g)$. And hence $C(\mu_1, \mu_2, k) \subseteq \Big\{F \in C(\mu_1, \mu_2) |\ F(\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} g \begin{pmatrix} a^{'} & b^{'} \\ c^{'} & d^{'} \end{pmatrix}) = \mu_1(a)\mu_2(b)\mu_1\mu_2(a^{'})F(g)$ $\forall\, g \in GL(2, \mathbb{Z}_p), \begin{pmatrix} a & x \\ 0 & b \end{pmatrix} \in B(\mathbb{Z}_p), \begin{pmatrix} a^{'} & b^{'} \\ c^{'} & d^{'} \end{pmatrix} \in \Gamma_0(k)\Big\}$. For the other inclusion, take an element in $\Big\{F \in C(\mu_1, \mu_2) |\ F(\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} g \begin{pmatrix} a^{'} & b^{'} \\ c^{'} & d^{'} \end{pmatrix}) = \mu_1(a)\mu_2(b)\mu_1\mu_2(a^{'})F(g)$ $\forall\, g \in GL(2, \mathbb{Z}_p), \begin{pmatrix} a & x \\ 0 & b \end{pmatrix} \in B(\mathbb{Z}_p), \begin{pmatrix} a^{'} & b^{'} \\ c^{'} & d^{'} \end{pmatrix} \in \Gamma_0(k)\Big\}$ and choose $\begin{pmatrix} a & x \\ 0 & b \end{pmatrix}$ to be the identity matrix I, and then we can easily see that $\Big\{F \in C(\mu_1, \mu_2) |\ F(\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} g \begin{pmatrix} a^{'} & b^{'} \\ c^{'} & d^{'} \end{pmatrix}) = \mu_1(a)\mu_2(b)\mu_1\mu_2(a^{'})F(g)$

$\forall\, g \in GL(2,\mathbb{Z}_p), \begin{pmatrix} a & x \\ 0 & b \end{pmatrix} \in B(\mathbb{Z}_p), \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \Gamma_0(k)\Big\} \subseteq C(\mu_1,\mu_2,k)$ which completes the proof. □

Lemma 4.0.16. *Given two quasi characters $\mu_1,\mu_2 : \mathbb{Q}_p^\times \to \mathbb{C}^\times$, then their product*

$$\mu_1\mu_2 : \mathbb{Q}_p^\times \to \mathbb{C}^\times,$$

is a quasi character.

Proof. It is easy to check that the product is a well defined function, a homomorphism and continuous, as we know what the topologies of $\mathbb{C}$ and $\mathbb{Q}_p$ are. □

Lemma 4.0.17. *Let n_0, n_1, n_2 denotes the conductors of $\mu_1\mu_2, \mu_1, \mu_2$ respectively then $n_0 \leq max(n_1, n_2)$.*

Proof. I claim that n_0 is actually equals to $\max(n_1,n_2)$ provided that $n_1 \neq n_2$ and n_0 might be less than $\max(n_1,n_2)$ if $n_1 = n_2$, so I will separate my proof into two cases:

Case (1): If $n_1 \neq n_2$ then without loss of generality assume $n_2 > n_1$, I will split this into two cases:

Case (a): If $n_1 = 0$ (μ_1 is trivial on $\mathbb{Z}_p^\times$) and $n_2 = 1$ then $\mu_1\mu_2|_{1+p\mathbb{Z}_p} = 1$. Hence, the conductor in this case is either zero or 1. Note that $\mu_1\mu_2|_{\mathbb{Z}_p^\times} = \mu_2|_{\mathbb{Z}_p^\times} \neq 1$. Therefore $\mu_1\mu_2$ is not trivial on $\mathbb{Z}_p^\times$, we conclude that $cond(\mu_1\mu_2) = 1 = \max(n_1,n_2)$.

Case (b): If n_1 is a non-negative integer and n_2 is greater than 1. Now, as $n_1 < n_2$ we have $n_1 < \max(n_1,n_2) = n_2$, therefore $n_2 \geq n_1 + 1$ and $n_2 \geq 2$. Now, since n_2 is the conductor of μ_2, then we have

$$\mu_2|_{1+p^{n_2}\mathbb{Z}_p} = 1.$$

If $n \geq n_2$ then $\mu_1\mu_2|_{1+p^n\mathbb{Z}_p} = 1.1 = 1$. Now, I should prove that n_2 is the least where

$$\mu_1\mu_2|_{1+p^{n_2}\mathbb{Z}_p} = 1.$$

For that, it is enough to show that $\mu_1\mu_2|_{1+p^{n_2-1}\mathbb{Z}_p} \neq 1$. Now, as we have $n_2 \geq n_1 + 1$ and $n_2 \geq 2$, then $n_2 - 1 \geq n_1$ and $n_2 - 1 \geq 1$, and so $\mu_1|_{1+p^{n_2-1}\mathbb{Z}_p} = 1$, but $\mu_2|_{1+p^{n_2-1}\mathbb{Z}_p} \neq 1$ (since $n_2 =$ conductor of μ_2) then $\mu_1\mu_2|_{1+p^{n_2-1}\mathbb{Z}_p} \neq 1$.

Case (2): If $n = n_1 = n_2$ then we have $\mu_1\mu_2|_{1+p^n\mathbb{Z}_p} = 1$, and then the conductor is this specific n or some non-negative integer less than n, for more details, I will split this case into two cases:

Case(a): If $\mu_1(a) = \frac{1}{\mu_2(a)}$ $\forall a \in 1 + \mathbb{Z}_p = \mathbb{Z}_p$, where $a \neq 0$, then we have $\mu_1\mu_2(a) = 1$ for all $a \in \mathbb{Z}_p^\times$. Hence, the conductor $n_0 = 0$ by definition.

Case(b): If there is some non-zero $a \in 1 + \mathbb{Z}_p = \mathbb{Z}_p$ such that $\mu_1(a) \neq \frac{1}{\mu_2(a)}$then consider the chain

$$\mathbb{Z}_p = 1 + \mathbb{Z}_p \supset 1 + p\mathbb{Z}_p \supset ... \supset 1 + p^{n-2}\mathbb{Z}_p \supset 1 + p^{n-1}\mathbb{Z}_p,$$

and then let i be the least positive integer in $\{1, 2, 3, 4, ..., n\}$ such that $\exists\ a \in 1 + p^{n-i}\mathbb{Z}_p$, where $\mu_1(a) \neq \frac{1}{\mu_2(a)}$, where such an i exists by assumption, then the conductor $n_0 = n - i + 1$. □

Lemma 4.0.18. *If $k < n_0$ then $C(\mu_1, \mu_2, k) = 0$.*

Proof. Suppose $k < n_0$, then $\mu_1\mu_2|_{1+p^k\mathbb{Z}_p} \neq 1$, then $\exists\ a \in \mathbb{Z}_p$ such that $\mu_1\mu_2(1 + p^k a) \neq 1$. Consider the matrix $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. Let $F \in C(\mu_1, \mu_2, k)$, then we have to show that $F(g) = 0$ for all $g \in GL(2, \mathbb{Z}_p)$. Let $g \in GL(2, \mathbb{Z}_p)$, then consider $F(g \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p^k & 1 \end{pmatrix}) = F(g \begin{pmatrix} 1 + ap^k & a \\ p^k & 1 \end{pmatrix} = \mu_1\mu_2(1 + ap^k)F(g)$. On the other hand, let $g' = g \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ then $F(g \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p^k & 1 \end{pmatrix}) = F(g' \begin{pmatrix} 1 & 0 \\ p^k & 1 \end{pmatrix}) = F(g') = F(g \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = F(g)$. Therefore, we have $F(g) = \mu_1\mu_2(1 + p^k a)F(g)$, where $\mu_1\mu_2(1 + p^k a) \neq 1$, we conclude that

$F(g) = 0$, and since g is arbitrarily chosen from $GL(2, \mathbb{Z}_p)$, then $F = 0$. Now, as F is arbitrarily chosen from $C(\mu_1, \mu_2, k)$, then $C(\mu_1, \mu_2, k) = 0$. □

Now, from the previous lemma, we can conclude that if $C(\mu_1, \mu_2, k) \neq 0$ then we have $k \geq n_0 =$ conductor of $\mu_1\mu_2$. The following theorem actually says more, it says that if $C(\mu_1, \mu_2, k) \neq 0$ then $k \geq \max(n_1, n_2) \geq n_0$, but first, we will state and prove some lemmas.

Lemma 4.0.19. *If $k \geq n_0$ then $C(\mu_1, \mu_2, k) \subset R(B(\mu_1, \mu_2)^{K(p^k)})$.*

Proof. First note that the space $R(B(\mu_1, \mu_2)^{K(p^k)})$ is the space of all functions F such that $F = R(f)$, where $f \in B(\mu_1, \mu_2)$ satisfying $f(xk') = f(x)$ for each $x \in GL(2, \mathbb{Q}_p)$, $k' \in K(p^k)$, or equivalently, it is the space of all functions F such that $F(xk') = F(x)$ for each $x \in GL(2, \mathbb{Z}_p)$, $k' \in K(p^k)$. Now, let $G \in C(\mu_1, \mu_2, k)$, then by definition of $C(\mu_1, \mu_2, k)$ we have

$$G(x \begin{pmatrix} a & b \\ c & d \end{pmatrix}) = \mu_1(a)\mu_2(a)G(x),$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(k), x \in GL(2, \mathbb{Z}_p)$. Now, as $K(p^k) \subseteq \Gamma_0(k)$, then

$$G(x \begin{pmatrix} a & b \\ c & d \end{pmatrix}) = \mu_1(a)\mu_2(a)G(x),$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K(p^k), x \in GL(2, \mathbb{Z}_p)$. Now, if $k' = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K(p^k)$ then by definition of $K(p^k)$ we have $a \equiv 1 \bmod(p^k)$, and as $k \geq n_0$, we conclude that $\mu_1\mu_2(a) = 1$. Hence, $G(xk') = \mu_1\mu_2(a)G(x) = 1.G(x) = G(x)$. Therefore, $G \in R(B(\mu_1, \mu_2)^{K(p^k)})$ which completes the proof. □

Lemma 4.0.20. *let n_0, n_1, n_2 denote the conductors of $\mu_1\mu_2, \mu_1, \mu_2$ respectively, then*

$$C(\mu_1, \mu_2, k) \neq 0 \Rightarrow k \geq max(n_1, n_2) \geq n_0.$$

Proof. let n_0, n_1, n_2 denote the conductors of $\mu_1\mu_2, \mu_1, \mu_2$ respectively and assume that $C(\mu_1, \mu_2, k) \neq 0$. Now, in lemma 4.0.17 we proved that $\max(n_1, n_2) \geq n_0$. Further, if we have $\max(n_1, n_2) = n_0$ then we are done by lemma 4.0.18. By lemma 3.5.7, we have that if $k <\max(n_1, n_2)$ then $V(\chi_1, \chi_2)^{K(p^k)} = 0$, and as we have $B(\mu_1, \mu_2) = V(\chi_1, \chi_2)$, then we have $B(\mu_1, \mu_2)^{K(p^k)} = 0$. This implies that $R(B(\mu_1, \mu_2)^{K(p^k)}) = 0$. But we proved in the previous lemma that if $k \geq n_0$ then $C(\mu_1, \mu_2, k) \subset R(B(\mu_1, \mu_2)^{K(p^k)}) = 0$, which completes the proof. □

Therefore, we have proved that if $V(\rho, k)$ is nontrivial then $k \geq \max(n_1, n_2)$.

Remark. Suppose that we have the groups W, G and H is a subgroup of G. Furthermore, suppose that $\phi : G \to W$ is a homomorphism. We want to determine under which restrictions we can define a homomorphism $\phi' : G/H \to W$ by

$$\phi'(aH) = \phi(a).$$

For the previous function to be well-defined we must have $\phi'(aH) = \phi'(bH)$ provided that $aH = bH$ or $b^{-1}a \in H$. Note that a homomorphism ϕ' satisfies $\phi'(aH) = \phi'(bH)$ if and only if $\phi(b^{-1}aH) = e_W$ (where $= e_W$ denotes the identity element in the group W) and as $b^{-1}a \in H$ this is equivalent to saying that $\phi'(H) = e_W$ or $\phi(h) = e_W$ for all $h \in H$. Hence, for ϕ' to be well-defined, all the elements in the subgroup H must map to the identity in W. In particular, we have the homomorphisms $\mu_1, \mu_2, \mu_1\mu_2$ restricted on $\mathbb{Z}_p^\times$. Then, if $k \geq \max(cond(\mu_1), cond(\mu_2))$ we have $\mu_1, \mu_2, \mu_1\mu_2|_{1+p^k\mathbb{Z}_p} = 1$. Hence, we can define a new $\mu_1, \mu_2, \mu_1\mu_2 : \mathbb{Z}_p^\times/1 + p^k\mathbb{Z}_p \to \mathbb{C}^\times$ by $\mu_1(a(1 + p^k\mathbb{Z}_p)) = \mu_1(a)$, $\mu_2(a(1 + p^k\mathbb{Z}_p)) = \mu_2(a)$ and $\mu_1\mu_2(a(1 + p^k\mathbb{Z}_p)) = \mu_1\mu_2(a)$. Now, as we have $\mathbb{Z}_p^\times/1 + p^k\mathbb{Z}_p \cong (\mathbb{Z}_p/p^k\mathbb{Z}_p)^\times$, then we can define $\mu_1, \mu_2, \mu_1\mu_2$ on $(\mathbb{Z}_p/p^k\mathbb{Z}_p)^\times$ instead.

Definition. The set $D(\mu_1, \mu_2, k)$ is defined to be the set of all functions

$\phi : GL(2, \mathbb{Z}_p/p^k\mathbb{Z}_p) \to \mathbb{C}$ satisfying

$$\phi(\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} g \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}) = \mu_1(a)\mu_2(b)\mu_1\mu_2(a')\phi(g),$$

$$\forall\, g \in GL(2, \mathbb{Z}_p/p^k\mathbb{Z}_p), \begin{pmatrix} a & x \\ 0 & b \end{pmatrix} \in B(\mathbb{Z}_p/p^k\mathbb{Z}_p), \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} \in B(\mathbb{Z}_p/p^k\mathbb{Z}_p).$$

Lemma 4.0.21. *We have*

$$C(\mu_1, \mu_2, k) \cong D(\mu_1, \mu_2, k).$$

Proof. I claim that the following function T is an isomorphism

$$T : C(\mu_1, \mu_2, k) \to D(\mu_1, \mu_2, k),$$

defined by

$$[T(F)](\overline{x}) = F(x),$$

where $F \in C(\mu_1, \mu_2, k)$, $x \in GL(2, \mathbb{Z}_p)$, $\overline{x} \in GL(2, \mathbb{Z}_p/p^k\mathbb{Z}_p)$ and $\overline{x}$ is the image of x mod(p^k). Lets first prove that T is well defined.

(1) To show that T is well defined

Let $x_1, x_2 \in GL(2, \mathbb{Z}_p)$ such that $\overline{x_1} = \overline{x_2} = \overline{x} \in GL(2, \mathbb{Z}_p/p^k\mathbb{Z}_p)$. We should show that $F(x_1) = F(x_2)$. Now, as $\overline{x_1} = \overline{x_2}$, then $\overline{x_1^{-1}x_2} = I$, and hence $x_1^{-1}x_2 = I + p^k m$, where m is a matrix with entries from $\mathbb{Z}_p$. Therefore, $x_1^{-1}x_2 \in K(p^k)$, then by lemma 4.0.19 we have $F(g(x_1^{-1}x_2)) = F(g)$, for all g in $GL(2, \mathbb{Z}_p)$. Choose $g = x_1$, then we get $F(x_2) = F(Ix_2) = F(x_1)$, we conclude that T is well defined.

(2) Lets show that T is linear:

(a) $T[(F + G)](\overline{x})) = (F + G)(x) = F(x) + G(x) = [T(F)](\overline{x}) + [T(G)](\overline{x})]$, where $x \in GL(2, \mathbb{Z}_p)$ and $\overline{x} \in GL(2, \mathbb{Z}_p/p^k\mathbb{Z}_P)$ where $\overline{x} = x$ mod(p^k).

(b) $[T(\alpha F)](\overline{x}) = (\alpha F)(x) = \alpha F(x) = \alpha[T(F)](\overline{x})$, where $x \in GL(2,\mathbb{Z}_p)$ and $\overline{x} \in GL(2,\mathbb{Z}_p/p^k\mathbb{Z}_P)$, where $\overline{x} = x \bmod(p^k)$.

(3) Lets now show that it is 1-1:

Lets assume we have two functions $F, G \in C(\mu_1,\mu_2,k)$ such that $[T(F)](\overline{x})) = [T(G)](\overline{x})$ at each $\overline{x} \in GL(2,\mathbb{Z}_p/p^k\mathbb{Z}_p)$, then we have $F(x) = [T(F)](\overline{x}) = [T(G)](\overline{x}) = G(x)$, and that is for all $x \in GL(2,\mathbb{Z}_p)$, hence $F = G$ and so T is 1-1.

(4) T is onto:

Let $\phi \in D(\mu_1,\mu_2,k)$, then

$$\phi(\begin{pmatrix} \overline{a} & \overline{x} \\ 0 & \overline{b} \end{pmatrix} \overline{g} \begin{pmatrix} \overline{a}' & \overline{b}' \\ 0 & \overline{d}' \end{pmatrix}) = \mu_1(\overline{a})\mu_2(\overline{b})\mu_1\mu_2(\overline{a}')\phi(\overline{g}),$$

for all $\begin{pmatrix} \overline{a} & \overline{x} \\ 0 & \overline{b} \end{pmatrix}, \begin{pmatrix} \overline{a}' & \overline{b}' \\ 0 & \overline{d}' \end{pmatrix} \in B(\mathbb{Z}_p/p^k\mathbb{Z}_p)$, $\overline{g} \in GL(2,\mathbb{Z}_p/p^k\mathbb{Z}_p)$. Define

$$F : GL(2,\mathbb{Z}_p) \to \mathbb{C},$$

by

$$F(g) = \phi(\overline{g}),$$

where $g \in GL(2,\mathbb{Z}_p)$. We have to show that $F \in C(\mu_1,\mu_2,k)$ and $T(F) = \phi$. Let's first show that $F \in C(\mu_1,\mu_2,k)$. Let $\begin{pmatrix} a & x \\ 0 & b \end{pmatrix}, \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in B(\mathbb{Z}_p), \Gamma_0(k)$ respectively, and let $g \in GL(2,\mathbb{Z}_p)$. Then, consider that $F(\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} g \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}) = \phi(\begin{pmatrix} \overline{a} & \overline{x} \\ 0 & \overline{b} \end{pmatrix} \overline{g} \begin{pmatrix} \overline{a'} & \overline{b'} \\ 0 & \overline{d'} \end{pmatrix}) = \mu_1(\overline{a})\mu_2(\overline{b})\mu_1\mu_2(\overline{a'})\phi(\overline{g})$. Now, as $\overline{a} = a \bmod(p^k)$, $\overline{b} = b \bmod(p^k)$, $\overline{a'} = a' \bmod(p^k)$, $a, b \in \mathbb{Z}_p^\times$ and $a' \in \mathbb{Z}_p^\times$, then $\mu_1(\overline{a}) = \mu_1(a), \mu_2(\overline{b}) = \mu_2(b)$

and $\mu_1\mu_2(\overline{a'}) = \mu_1\mu_2(a')$. But by definition of function F, we have $F(g) = \phi(\overline{g})$, hence $F(\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} g \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}) = \phi(\begin{pmatrix} \overline{a} & \overline{x} \\ 0 & \overline{b} \end{pmatrix} \overline{g} \begin{pmatrix} \overline{a'} & \overline{b'} \\ 0 & \overline{d'} \end{pmatrix}) = \mu_1(\overline{a})\mu_2(\overline{b})\mu_1\mu_2(\overline{a'})\phi(\overline{g}) = \mu_1(a)\mu_2(b)\mu_1\mu_2(a')F(g)$. Therefore, $F \in C(\mu_1, \mu_2, k)$. Now, let's show that $T(F) = \phi$. Note that for each $\overline{g} \in GL(2, \mathbb{Z}_p/p^k\mathbb{Z}_p)$ we have $[T(F)](\overline{g}) = F(g) = \phi(\overline{g})$ which completes the proof. □

Remark. According to what we have showed until now, it is enough for us to study the space $D(\mu_1, \mu_2, k)$ consisting of all functions $\phi : GL(2, \mathbb{Z}_p/p^k\mathbb{Z}_p) \to \mathbb{C}$ satisfying $\phi(\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} g \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}) = \mu_1(a)\mu_2(b)\mu_1\mu_2(a')\phi(g), \quad \forall\, g \in GL(2, \mathbb{Z}_p/p^k\mathbb{Z}_p), \begin{pmatrix} a & x \\ 0 & b \end{pmatrix} \in B(\mathbb{Z}_p/p^k\mathbb{Z}_p), \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} \in B(\mathbb{Z}_p/p^k\mathbb{Z}_p)$. Indeed, as we have $\mathbb{Z}_p/p^k\mathbb{Z}_p \cong \mathbb{Z}/p^k\mathbb{Z}$, then we can consider these functions ϕ on $GL(2, \mathbb{Z}/p^k\mathbb{Z})$ instead. Now, for the following lemmas, let's note that an element $a \in \mathbb{Z}_p/p^k\mathbb{Z}_p$ is a unit if and only if $gcd(a, p) = 1$, or, in other words, if and only if p does not divide a. Let's also remember that for an element $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to be in $GL(2, R)$, where R is any given commutative ring with unity, then we must have $ad - cb \in R^\times$,i.e., $ad - cb$ should be a unit in R.

Lemma 4.0.22. *Every element a in $\mathbb{Z}/p^k\mathbb{Z}$ can be written as*

$$a = bp^i,$$

where b is a unit and i is a unique element in $\{0, 1, 2, ..., k\}$.

Proof. Let $a \in \mathbb{Z}/p^k\mathbb{Z}$.

If a itself is unit then $a = ap^0$. Therefore, $i = 0$ in this case. Hence, assume a is not unit. Now, if a is not unit, we consider two cases:

(1) If $a = 0$ then $a = 1.p^k$, hence, $i = k$ in this case and then we are done.

(2) If $a \neq 0$, then $p|a$. Let i be the largest positive integers such that $p^i|a$, in other words, let i be the positive integer such that $p^i|a$ but $p^{i+1} \nmid a$ then we have $a = bp^i$, where $p \nmid b$ (as if $p|b$ then $p^{i+1}|a$). Hence, b is a unit. Here, as $a \neq 0$ then the possible values for i are $\{1, 2, ..., k-1\}$.

For uniqueness, suppose $ap^i = bp^j$ with a, b are units and $i, j \in \{1, 2, ..., k-1\}$ such that $i \geq j$ (without loss of generality). Now, multiply both sides by p^{k-i}, then you get zero in the left hand side and bp^{k-i+j} in the right hand side. Because the two sides are equal, we should have zero in the left hand side as well. Hence $p^{k-i+j} = p^k = 0$, and as $i, j \in \{1, 2, ..., k-1\}$ we must have $i = j$. □

Lemma 4.0.23. *Let g be an element of $GL(2, \mathbb{Z}/p^k\mathbb{Z})$, then g can be decomposed as*

$$g = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix},$$

where $\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} \in B(\mathbb{Z}/p^k\mathbb{Z}), \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} \in GL(2, \mathbb{Z}/p^k\mathbb{Z}).$

Proof. Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{Z}/p^k\mathbb{Z})$. I will split this prove into two cases:

Case(1): If d is a unit then $\begin{pmatrix} 1 & -bd^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a - cbd^{-1} & 0 \\ c & d \end{pmatrix}$, where $a - cbd^{-1}$ is unit as if $p|a - cbd^{-1}$ then $p|d(a - cbd^{-1}) = da - cb$ which can't occur as $da - cb$ is a unit. Therefore, we must have $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & bd^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a - cbd^{-1} & 0 \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ which completes the proof of case(1).

Case(2): If d is not a unit. First note that if d is not a unit then $p|d$, so c must be a unit, as if c is not a unit then p divides both d and c, hence $p|ad-bc$, so c is a unit. Now, $c+d$ is a unit, as if $p|c+d$ then p divides c. Now, note that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}$. Now, as $c+d$ is a unit we can apply case(1) on $\begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}$ and then we have $\begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = x\begin{pmatrix} * & 0 \\ * & * \end{pmatrix} y$, where $x, y \in B(\mathbb{Z}/p^k\mathbb{Z})$, and $\begin{pmatrix} * & 0 \\ * & * \end{pmatrix} \in GL(2, \mathbb{Z}/p^k\mathbb{Z})$. Hence, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = x\begin{pmatrix} * & 0 \\ * & * \end{pmatrix} y$, therefore

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = x\begin{pmatrix} * & 0 \\ * & * \end{pmatrix} y \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix},$$

and as both $y, \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \in B(\mathbb{Z}/p^k\mathbb{Z})$, then $y' = y\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \in B(\mathbb{Z}/p^k\mathbb{Z})$. Hence,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = x\begin{pmatrix} * & 0 \\ * & * \end{pmatrix} y',$$

where $x, y' \in B(\mathbb{Z}/p^k\mathbb{Z})$, $\begin{pmatrix} * & 0 \\ * & * \end{pmatrix} \in GL(2, \mathbb{Z}/p^k\mathbb{Z})$. □

Lemma 4.0.24. *For all*

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{Z}/p^k\mathbb{Z}),$$

there is a unique $i \in \{0, 1, 2, ..., k\}$ *such that*

$$g = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix},$$

for some $\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} \in B(\mathbb{Z}/p^k\mathbb{Z})$.

Proof. Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{Z}/p^k\mathbb{Z})$, then by previous lemma we can decompose g as $g = \begin{pmatrix} a_1' & b_1' \\ 0 & d_1' \end{pmatrix} \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} \begin{pmatrix} a_2' & b_2' \\ 0 & d_2' \end{pmatrix}$ where $\begin{pmatrix} a_1' & b_1' \\ 0 & d_1' \end{pmatrix} \begin{pmatrix} a_2' & b_2' \\ 0 & d_2' \end{pmatrix} \in B(\mathbb{Z}/p^k\mathbb{Z})$, $\begin{pmatrix} x & 0 \\ y & z \end{pmatrix} \in GL(2, \mathbb{Z}/p^k\mathbb{Z})$. Now, consider the matrix $\begin{pmatrix} x & 0 \\ y & z \end{pmatrix}$, as this matrix is in $GL(2, \mathbb{Z}/p^k\mathbb{Z})$, then x and z both must be units, and hence we have $\begin{pmatrix} 1 & 0 \\ 0 & z^{-1} \end{pmatrix} \begin{pmatrix} x^{-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ z^{-1}y & 1 \end{pmatrix}$. Because $z^{-1}y \in \mathbb{Z}/p^k\mathbb{Z}$, then by lemma 4.0.22, we can write $z^{-1}y$ as $z^{-1}y = bp^i$, and hence $\begin{pmatrix} 1 & 0 \\ z^{-1}y & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ bp^i & 1 \end{pmatrix}$. Now, note that we have $\begin{pmatrix} b & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ bp^i & 1 \end{pmatrix} \begin{pmatrix} b^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix}$, hence $\begin{pmatrix} b & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix} \begin{pmatrix} b^{-1} & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ bp^i & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ z^{-1}y & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & z^{-1} \end{pmatrix} \begin{pmatrix} x^{-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & 0 \\ y & z \end{pmatrix}$, therefore $\begin{pmatrix} x & 0 \\ y & z \end{pmatrix} = \begin{pmatrix} x^{-1} & 0 \\ 0 & 1 \end{pmatrix}^{-1}$

$\begin{pmatrix} 1 & 0 \\ 0 & z^{-1} \end{pmatrix}^{-1} \begin{pmatrix} b & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix} \begin{pmatrix} b^{-1} & 0 \\ 0 & 1 \end{pmatrix}^{-1}$. As $B(\mathbb{Z}/p^k\mathbb{Z})$ is subgroup, then we can these matrices together where the result is an upper triangular matrix as well. Thus, we can say that $\begin{pmatrix} x & 0 \\ y & z \end{pmatrix} = \begin{pmatrix} g_1 & g_2 \\ 0 & g_3 \end{pmatrix}$ $\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & b^{-1} \end{pmatrix}$, where $\begin{pmatrix} g_1 & g_2 \\ 0 & g_3 \end{pmatrix} \in B(\mathbb{Z}/p^k\mathbb{Z})$, therefore $g = \begin{pmatrix} a_1' & b_1' \\ 0 & d_1' \end{pmatrix} \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} \begin{pmatrix} a_2' & b_2' \\ 0 & d_2' \end{pmatrix} = \begin{pmatrix} a_1' & b_1' \\ 0 & d_1' \end{pmatrix} \begin{pmatrix} g_1 & g_2 \\ 0 & g_3 \end{pmatrix}$ $\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & b^{-1} \end{pmatrix} \begin{pmatrix} a_2' & b_2' \\ 0 & d_2' \end{pmatrix}$ and as $B(\mathbb{Z}/p^k\mathbb{Z})$ is subgroup, we can multiply terms and still get elements in $B(\mathbb{Z}/p^k\mathbb{Z})$. Now, for uniqueness, assume that we have $g = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} = \begin{pmatrix} a_1' & b_1' \\ 0 & d_1' \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p^j & 1 \end{pmatrix} \begin{pmatrix} a_2' & b_2' \\ 0 & d_2' \end{pmatrix}$, then $\begin{pmatrix} a_1 {a_1'}^{-1} & * \\ 0 & d_1 {d_2'}^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ p^j & 1 \end{pmatrix} \begin{pmatrix} a_2^{-1}a_2' & * \\ 0 & d_2^{-1}d_2' \end{pmatrix}$. Hence, $x = p^j a_2^{-1} a_2' = p^i d_1 {d_2'}^{-1} \in \mathbb{Z}/p^k\mathbb{Z}$ where $a_2^{-1}a_2', d_1{d_2'}^{-1}$ are units in $\mathbb{Z}/p^k\mathbb{Z}$, then by lemma 4.0.22 we have $i = j$ which completes the proof. □

Corollary 4.0.25. *We have*

$$GL(2, \mathbb{Z}/p^k\mathbb{Z}) = \bigcup_{0 \le i \le k} B(\mathbb{Z}/p^k\mathbb{Z}) \begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix} B(\mathbb{Z}/p^k\mathbb{Z}),$$

where these double cosets are distinct.

Proof. The proof follows immediately from the previous lemma. □

Remark. By the previous lemma, and by definition of the space $D(\mu_1, \mu_2, k)$, a function $\phi \in D(\mu_1, \mu_2, k)$ is completely determined on its values on the matrices $\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix}$, where $i \in \{0, 1, 2, ..., k\}$. Now, what I am going to do next is to show that not all of these $k+1$ values are free. Some of them have to be zero. Furthermore, we will prove that if $D(\mu_1, \mu_2, k)$ is not trivial then $k \geq cond(\mu_1) + cond(\mu_2)$.

Lemma 4.0.26. *Given $a, a', b, b' \in \mathbb{Z}/p^k\mathbb{Z}$, there exists $x, x' \in \mathbb{Z}/p^k\mathbb{Z}$ such that* $\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix} \begin{pmatrix} a' & x' \\ 0 & b' \end{pmatrix}$ *if and only if*

$$b \equiv b' \ mod(p^i),$$

$$a \equiv a' \ mod(p^i),$$

$$a' \equiv b \ mod(p^{k-i}),$$

$$b - b' = a' - a.$$

Proof. ($\Rightarrow$) Given $a, a', b, b' \in \mathbb{Z}/p^k\mathbb{Z}$, then by assumption there exists $x, x' \in \mathbb{Z}/p^k\mathbb{Z}$ such that $\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix} \begin{pmatrix} a' & x' \\ 0 & b' \end{pmatrix}$, hence we have:

(1) $a + xp^i = a'$,

(2) $x = x'$,

(3) $bp^i = a'p^i$,

(4) $b = b' + x'p^i$,

where all these equalities are mod(p^k). Now, from (1) and (4) we can directly conclude that

$$b \equiv b' \ \text{mod}(p^i),$$

$$a \equiv a' \ \text{mod}(p^i).$$

For (3), as I have mentioned, all these equalities are mod(p^k), hence what (3) actually says is that: $bp^i = a^{'}p^i + k_1p^k$ for some $k_1 \in \mathbb{Z}/p^k\mathbb{Z}$ or $b = a^{'} + k_1p^{k-i}$, therefore we have $b \equiv a^{'}$ mod(p^{k-i}). For (2), as $x = x^{'}$, then $p^ix = p^ix^{'}$, then by (1) and (4) we have $b - b^{'} = a^{'} - a$ which completes the proof in this direction.

($\Leftarrow$) Given $a, a^{'}, b, b^{'} \in \mathbb{Z}/p^k\mathbb{Z}$ such that

$$b \equiv b^{'} \mod(p^i),$$

$$a \equiv a^{'} \mod(p^i),$$

$$a^{'} \equiv b \mod(p^{k-i}),$$

$$b - b^{'} = a^{'} - a,$$

then we have (all mod(p^k)):

(1) $b = b^{'} + k_1p^i$,

(2) $a^{'} = a + k_2p^i$,

(3) $a^{'} = b + k_3p^{k-i}$,

(4) $b - b^{'} = a^{'} - a \Rightarrow k_1p^i = k_2p^i$, where $k_1, k_2, k_3 \in \mathbb{Z}/p^k\mathbb{Z}$. As from (4) we have $k_1p^i = k_2p^i$, then we can rewrite the first equation as $b = b^{'} + k_2p^i$. Now, let $x^{'} := k_2$ and $x := k_2$, then these four equations are (all mod(p^k)):

(1) $b = b^{'} + x^{'}p^i$,

(2) $a^{'} = a + xp^i$,

(3) $a^{'}p^i = bp^i$,

and by our choice of $x^{'}$, x we have $x^{'} = x$.

We conclude that the equation

$$\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix} \begin{pmatrix} a^{'} & x^{'} \\ 0 & b^{'} \end{pmatrix},$$

is satisfied.

□

Lemma 4.0.27. *If $i < n_1$ then $\forall \phi \in D(\mu_1, \mu_2, k)$, we have $\phi(\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix}) = 0$.*

Proof. Suppose $i < n_1 = \text{cond}(\mu_1)$, then the there exists $a, \overline{a} \in (\mathbb{Z}_p/p^k\mathbb{Z}_p)^\times$ such that $a \equiv \overline{a} \mod(p^i)$, but $\mu_1(a) \neq \mu_1(\overline{a})$, hence $\overline{a} = a + xp^i$ where $x \in \mathbb{Z}_p/p^k\mathbb{Z}_p$ and $\mu_1(a) \neq \mu_1(\overline{a})$. Then, note that $\begin{pmatrix} a & x \\ 0 & \overline{a} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix}\begin{pmatrix} \overline{a} & x \\ 0 & a \end{pmatrix}$, but $\mu_1(a)\mu_2(\overline{a})\phi(\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix}) = \phi(\begin{pmatrix} a & x \\ 0 & \overline{a} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix}) = \phi(\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix}\begin{pmatrix} \overline{a} & x \\ 0 & a \end{pmatrix}) = \mu_1(\overline{a})\mu_2(\overline{a})\phi(\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix})$ and hence $\phi(\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix}) = 0$.

□

Lemma 4.0.28. *If $i > k - n_2$ then $\forall \phi \in D(\mu_1, \mu_2, k)$ we have $\phi(\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix}) = 0$.*

Proof. Suppose $i > k - n_2$, then $k - i < n_2$, hence there exists $b, a' \in (\mathbb{Z}_p/p^k\mathbb{Z}_p)^\times$ such that $b \equiv a' \mod(p^{k-i})$, but $\mu_2(b) \neq \mu_2(a')$, so $a' = b + xp^{k-i}$ where $x \in \mathbb{Z}_p/p^k\mathbb{Z}_p$ and $\mu_2(b) \neq \mu_2(a')$. Now, as we have $a' = b + xp^{k-i}$, then we get $p^i a' = p^i b$ (as all is mod (p^k)). Now, note that $\begin{pmatrix} a' & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix}\begin{pmatrix} a' & 0 \\ 0 & b \end{pmatrix}$, hence $\mu_1(a')\mu_2(b)$ $\phi(\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix}) = \phi(\begin{pmatrix} a' & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix}) = \phi(\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix}\begin{pmatrix} a' & 0 \\ 0 & b \end{pmatrix})$ $= \mu_1(a')\mu_2(a')\phi(\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix})$ and so $\phi(\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix}) = 0$. □

Remark. Note that from the previous two lemmas, in order to define a non-zero elements of $D(\mu_1, \mu_2, k)$, we should have $i \geq n_1$ and $k - i \geq n_2$. As a result, we should have

$k \geq n_1 + n_2$. Given $k \geq n_1 + n_2$, then the functions ϕ can have a non-zero only on those double cosets $B(\mathbb{Z}_p/p^k\mathbb{Z}_p)\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix} B(\mathbb{Z}_p/p^k\mathbb{Z}_p)$ where $n_1 \leq i \leq k-n_2$. I will states these results as corrollaries.

Corollary 4.0.29. *If $\phi \in D(\mu_1, \mu_2, k)$, then ϕ can be nonzero only on those double cosets where $i \geq n_1$ and $k - i \geq n_2$.*

Corollary 4.0.30. *If $k < n_1 + n_2$, then $D(\mu_1, \mu_2, k) = 0$.*

Remark. Note that the previous lemma does not tell us that we are guaranteed to have functions ϕ with a nonzero values on the cosets where $n_1 \leq i \leq k - n_2$. And that is what the next theorem is for.

Theorem 4.0.31. *Let $k \geq n_1 + n_2$ and let i be such that $n_1 \leq i \leq k - n_2$. Then if $g = \begin{pmatrix} a & x \\ 0 & b \end{pmatrix}\begin{pmatrix} 1 & 0 \\ p^j & 1 \end{pmatrix}\begin{pmatrix} \overline{a} & \overline{x} \\ 0 & \overline{b} \end{pmatrix} \in GL(\mathbb{Z}_p/p^k\mathbb{Z}_p)$ where $0 \leq j \leq k$, we have*

$$\phi_i(g) = \begin{cases} \mu_1(a)\mu_2(b)\mu_1\mu_2(\overline{a}) & : j = i \\ 0 & : j \neq i \end{cases}$$

is a well-defined function of $D(\mu_1, \mu_2, k)$.

Proof. Let

$$g = \begin{pmatrix} a_1 & x_1 \\ 0 & b_1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix}\begin{pmatrix} a_1' & x_1' \\ 0 & b_1' \end{pmatrix} = \begin{pmatrix} a_2 & x_2 \\ 0 & b_2 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix}\begin{pmatrix} a_2' & x_2' \\ 0 & b_2' \end{pmatrix}.$$

Then we have

$$\begin{pmatrix} a_1a_2^{-1} & * \\ 0 & b_1b_2^{-1} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix}\begin{pmatrix} a_2'a_1'^{-1} & * \\ 0 & b_2'b_1'^{-1} \end{pmatrix}.$$

Hence, by lemma 4.0.26, we have $a_1a_2^{-1} = a_2^{'}{a_1^{'}}^{-1} \bmod(p^i)$, and $b_1b_2^{-1} = a_2^{'}{a_1^{'}}^{-1} \bmod(p^{k-i})$. Then, as we have $i \geq n_1$ then $\mu_1(a_1a_2^{-1}) = \mu_1(a_2^{'}{a_1^{'}}^{-1})$, and as $k - i \geq n_2$, then we have $\mu_2(b_1b_2^{-1}) = \mu_2(a_2^{'}{a_1^{'}}^{-1})$, therefore

$$\mu_1(a_1)\mu_1(a_1^{'}) = \mu_1(a_2^{'})\mu_1(a_2), \quad \mu_2(b_1)\mu_2(a_1^{'}) = \mu_2(a_2^{'})\mu_2(b_2),$$

and then multiply the last two equations by each others left side by left side and right side by right side to get

$$\mu_1(a_1)\mu_2(b_1)\mu_1\mu_2(a_1^{'}) = \mu_1(a_2)\mu_2(b_2)\mu_1\mu_2(a_2^{'}) = \phi_i(g).$$

We conclude that ϕ_i is well defined. □

Theorem 4.0.32. *Let $k \geq n_1 + n_2$, then the set $\{\phi_i$ where $n_1 \leq i \leq k - n_2\}$ is basis for the space $D(\mu_1, \mu_2, k)$, and hence dim($D(\mu_1, \mu_2, k)$)$= k - n_2 - n_1 + 1$.*

Proof. Lets first show that the set $\{\phi_i$ where $n_1 \leq i \leq k - n_2\}$ is actually a spanning set for $D(\mu_1, \mu_2, k)$. Let $\phi \neq 0 \in D(\mu_1, \mu_2, k)$. Define $h := \sum_{i=n_1}^{k-n_2} \phi(\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix})\phi_i$.
I claim that $h(g) = \phi(g)$ for all $g \in GL(2, \mathbb{Z}/p^k\mathbb{Z})$. Let $g \in GL(2, \mathbb{Z}/p^k\mathbb{Z})$, then $g = \begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix}\begin{pmatrix} b_1 & b_2 \\ 0 & b_3 \end{pmatrix}$. Now, if $i \notin \{n_1, n_1 + 1, ..., k - n_2 - 1, k - n_2\}$, then by corrolary 4.0.29 and definition of ϕ_i we have $\phi(g) = 0$ and $\phi_i(g) = 0$, hence $h(g) = \phi(\begin{pmatrix} 1 & 0 \\ p^{n_1} & 1 \end{pmatrix})\phi_{n_1}(g) + \phi(\begin{pmatrix} 1 & 0 \\ p^{n_1+1} & 1 \end{pmatrix})\phi_{n_1+1}(g) + ... + \phi(\begin{pmatrix} 1 & 0 \\ p^{k-n_2} & 1 \end{pmatrix})\phi_{k-n_2}(g) = 0 + 0 + ... + 0 = 0$. Now, if $i \in \{n_1, n_1 + 1, ..., k - n_2 - 1, k - n_2\}$, then $\phi(g) = \mu_1(a_1)\mu_2(a_3)\mu_1\mu_2(b_1)\phi(\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix}) = \phi_i(g)\phi(\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix}) = \phi(\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix})\phi_i(g) = 0 + 0 + ... + \phi(\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix})\phi_i(g) + 0 + ... + 0 =$

$\sum_{j=n_1}^{k-n_2} \phi(\begin{pmatrix} 1 & 0 \\ p^j & 1 \end{pmatrix})\phi_j(g) = h(g)$, and since g is arbitrary, then $\phi = h$. Hence, the set $\{\phi_i$ where $n_1 \leq i \leq k - n_2\}$ is a spanning set for $D(\mu_1, \mu_2, k)$.

Now, to show that this set is linearly independent, suppose that

$$\sum_{i=n_1}^{k-n_2} c_i\phi_i = 0.$$

We should show that $c_i = 0$ for all $i \in \mathbb{Z}$ with $\in n_1 \leq i \leq k - n_2$. Let $i \in \mathbb{Z}$ with $n_1 \leq i \leq k - n_2$, then evaluate the given sum at the matrix $\begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix}$ to get

$0 + 0 + ... + c_i\phi_i(I \begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix} I) + 0 + 0 + ... + 0 = 0$, hence $c_i\mu_1(1)\mu_2(1)\mu_1\mu_2(1) = 0$, thus $c_i = 0$. Since, i is chosen arbitrarily from $\{n_1, n_1+1, ..., k-n_2-1, k-n_2\}$, then that is true for all i in this set. Therefore, the set $\{\phi_i$ where $n_1 \leq i \leq k - n_2\}$ is linearly independent. We conclude that the set $\{\phi_i$ where $n_1 \leq i \leq k - n_2\}$ is a basis for $D(\mu_1\mu_2, k)$. Thus, $\dim(D(\mu_1\mu_2, k)) = k - n_2 - n_1 + 1$.

□

REFERENCES

[1] Casselman, W., *On some results of atkin and lehner*, Math. Ann., (1973), pp. 301-314.

[2] Herwig, T. C., *The p-adic completion of* $\mathbb{Q}$ *and hensel's lemma*, (2011)8-26.

[3] Munkres, J. R., *Topology*, second edition, (2000)

[4] Cassels, J.W.S., Frohlich, A., *Algebraic Number Theory*, (1967) pp. 47-50.

[5] Weil, A., *Basic number theory*, Classics in mathematics, (1995), pp. 4

[6] Goldfeld, D., Hundley, J. *Automorphic Representations and L-Functions for the General linear Group*, Cambridge studies in advanced mathematics, (2011), Volume 1 pp. 1-5.

VITA

Graduate School
Southern Illinois University

Abdalrazzaq Zalloum Date of Birth: September 6, 1990

521 and 1/2 south illinois avenue, Carebondale, Illinois 62901

email address (zalloum@siu.edu)

Southern Illinois University at Carbondale
Bachelor of Science, Mathematics, August 20

Research Paper Title: PRINCIPAL SERIES REPRESENTATIONS OF $GL(2, \mathbb{Q}_p)$, AND THEIR CONDUCTORS AND NEWFORMS

Major Professor: Dr. Joseph Hundley